Jericho Forum

Visioning White Paper

What is Jericho Forum?

February 2005

This White Paper was prepared by Nick Bleech of KPMG with contributions from the Meta-Architecture Working Group of the Jericho Forum (Gary Yelland of Airbus, Steve Purser of Clearstream, Steve Greenham of GSK, Shane Tully of Qantas, John Walsh of ING and David Gracey of Rolls-Royce) and additional contributions from Paul Dorey of BP, Andrew Yeomans of Dresdner Kleinwort Wasserstein, Adrian Seccombe of Eli Lilly, Ian Dobson of The Open Group and David Lacey of Royal Mail.

Additional dialogue with representatives of the following organisations is also gratefully acknowledged: BT plc. nCipher Corporation Ltd., University of Kent, University of Auckland, New Zealand Police, Australian Government Information Management Office, Netsafe, KPMG (UK) LLP, Information Security Forum, and International Information Integrity Institute (I-4).

Contents

1 Executive Summary

Jericho Forum aims to develop and influence information and communications technology (ICT) security standards. These will facilitate the secure interoperation of ICT to support collaboration and commerce over open networks, within and between organisations, based on a security architecture and design approach entitled ***de-perimeterisation***.

This document sets out Jericho Forum's vision, mission and intended roadmap for de-perimeterisation. Its purpose is to inform members and the wider public what Jericho Forum is about (its rationale) and does (its mode of operation).

Jericho Forum brings together a variety of organisations in public and private sectors, academia, and interested individuals. The common factor is that they realise that some traditional approaches to network and system security architecture and design cannot cope with some important contemporary business drivers for collaboration and commerce. These include:

- Increasing on-line collaboration and trading among multiple business entities, which involve sharing sensitive and critical information
- Global trends towards accelerated outsourcing and offshoring of support services, core business processes and the skills sets that support them
- Use of low cost open networks to achieve collaboration and commerce.

There are universal needs to reduce ICT expenditure and improve infrastructure cost effectiveness, and encompass both traditional organisations and dynamic, looser structures.

De-perimeterisation is essentially about redesigning the security perimeters at the boundaries between an organisation's own ICT infrastructure/services and the open networks, individuals and other organisations with which it connects. Jericho Forum will formulate standards and guidance to help vendors to produce security technology that will interoperate effectively, and customer organisations to adopt technology and solutions to achieve de-perimeterisation.

Jericho Forum envisages that adopting de-perimeterisation will have a positive impact on end users and business stakeholders. It will consider a wide variety of business scenarios to illustrate relevant issues these stakeholders face today and will face in the future.

Jericho Forum has identified several areas needed to achieve its vision and mission, and it has established Working Groups to focus its work.

Jericho Forum recognises the important work other standards groups are undertaking and seeks to build on this where appropriate. It will influence relevant standards that are underway, and create new standards only where no other body can do so. It will focus on demonstrating that the standards it influences or develops actually deliver benefits to organisations. This will involve practical projects to build and demonstrate proofs of concept and pilot implementations, thus ensuring that standards are practical, cost effective, testable, evolvable and robust.

Jericho Forum encourages participation and dialogue, and this document concludes with membership information to enable organisations and individuals to get involved. Jericho Forum will depend on voluntary effort from the membership, but to ensure the progression of its vision and mission it will obtain funding via membership subscriptions and project grants.

2 Why the Need for Jericho Forum?

2.1 *Introduction – the need for change*

Jericho Forum believes that current information and communications technology (ICT) and the way security is organised as a series of concentric walls or layers around an organisation's private network perimeters and boundaries will need to change, perhaps radically, in the twenty-first century. The need for change, and evolution thereafter, arises in three ways.

Demand for open networks

Firstly, security, particular when operating in the corporate and government sectors, must recognise emerging business drivers for low cost collaboration and commerce over open networks and interfaces. Open networks include the public Internet as well as shared network services, which organisations can rent on demand, so reducing fixed costs and improving connectivity with employees, customers, business partners, suppliers and other external parties. As connectivity requirements increase (potentially from anywhere geographically in the world) to support greater collaboration and commerce:

- Uniform, simple and flexible access methods are needed for all types of collaboration and commerce
- Extending existing, private networks to meet new connectivity requirements is becoming too expensive
- Security controls that need to be changed, simply because of distance, access method, or constraints imposed by existing network structures and security perimeters, fundamentally limit the organisation's ability to meet its objectives.

These drivers already exist in the academic and 'home office' communities, where knowledge workers find it increasingly productive and efficient to collaborate and engage in commerce via open networks.

Infrastructure fragmentation

Secondly, the ability to create, deploy, secure, support and evolve an organisation's ICT infrastructure to support the organisation's business workload cost effectively will become more challenging as:

- It becomes more physically dispersed and also more interconnected (for example, via open networks)
- Ownership of infrastructure that underpins inter-organisational commerce or collaboration is more widely distributed among the constituents, and with outsourced service providers
- The task of managing and controlling each element of the extended infrastructure becomes increasingly complex.
- Organisations collaborate and deal increasingly with individuals operating in both a personal role (for example: in their capacity as consumer) and professional roles (for example: academic researchers, specialist contract workers based in home offices).

Individual-centric security

Thirdly, the need to secure individuals' access to and use of information within, on behalf of and between organisations is gaining more recognition. This places an increased emphasis on:

- Correctly validating and managing the logical identities individuals use for this access, and
- Demonstrating individuals' accountability for the access rights that they exercise.

Analysis

Jericho Forum believes that existing security approaches are a barrier to change because they assume:

- an organisation owns, controls and is accountable for the ICT infrastructure it employs (for example, this is a pervasive assumption in policy management systems), and
- all individuals sit within organisations (for example, this is a pervasive assumption in identity and access management (IAM) systems).

The approaches cannot cope with the dispersion, individual accountability, interconnection and fragmented ownership of infrastructure, accountability and access rights that are increasingly required.

Jericho Forum believes that a new security approach, entitled ***de-perimeterisation***, is required. De-perimeterisation affects the technology used for collaboration and commerce, but its impact goes further, because it encompasses the whole ICT lifecycle, from initial analysis of business goals through to eventual business and systems operation.

2.2 *Jericho Forum's Vision and Mission*

This section sets out Jericho Forum's formal Vision Statement, Mission Statement, and Timetable, together with key themes that elaborate upon the vision and mission statements.

Vision statement

To enable business confidence for collaboration and commerce beyond the constraint of the corporate, government, academic and home office perimeter, principally through:

- Cross-organisational security processes and services
- ICT products that conform to open security standards
- Assurance processes that when used in one organisation can be trusted by others.

Mission statement

Act as a catalyst to accelerate the achievement of the collective vision, by:

- Defining the problem space
- Communicating the collective vision
- Challenging constraints and creating an environment for innovation
- Demonstrating the market

- Influencing future products and standards.

Timetable

A period of three to five years for the achievement of Jericho Forum's vision, whilst accepting that its mission will continue beyond that.

Theme: developing security principles and standards

Jericho Forum will act as a catalyst for de-perimeterisation by driving the creation, convergence, endorsement and adoption of security principles and standards, so that:

- ICT buyers and users can be confident that Jericho Forum security principles and standards can be adopted at optimum cost and effectiveness in a given business context
- ICT product and solution vendors can be confident of an open commercial market for Jericho Forum standards-conformant ICT products and solutions, as well as the services that support, operate, manage or use them.

There will be a strong practical focus to Jericho Forum's standards development. Many existing standards in this field are poorly specified, ambiguous, and difficult to understand and validate.

Theme: enabling adoption

Jericho Forum recognises that de-perimeterisation may appear radical, and there is more to enabling change than standardising relevant vendor technology. Organisations will also need appropriate guidance on:

- Governance issues: how organisations should prepare for and guide de-perimeterisation, including consideration of interoperability with other organisations
- Strategic contexts: understanding relevant business drivers and requirements, as well as the principles, techniques and processes to turn business requirements into solution designs
- Requirements frameworks: common languages to express de-perimeterisation goals, requirements, policies, and solutions
- Business frameworks for collaboration and commerce between organisations: defining required trust relationships and assurance
- Security frameworks: defining security requirements in a standard way by classifying all elements involved in collaboration and commerce that may bear upon de-perimeterisation
- Design frameworks: addressing security architecture and design holistically for all ICT elements required
- Implementation and operation: defining relevant roles and responsibilities.

Theme: building consensus

Jericho Forum will work with other standards bodies, vendors and service providers as discussed further below. It will involve academia to help to ensure its security principles and standards are technically well founded, and engage in fundamental research if required. It will also engage with business and security forums and interest groups, to both capture their inputs and promote awareness of its activities and deliverables. It will ensure a strong practical focus for its work: demonstrable solutions are more useful to its membership than 'paper systems'.

Theme: fostering community

Jericho Forum is not just about developing standards-based solutions and problem solving. It will also act as a peer group for sharing security knowledge and experience, developing a network of people that can find the answers to questions on the topics within its scope, and to ensure that its results are practical and applicable to real organisations.

2.3 *Jericho Forum's Constituency*

Types of member

Jericho Forum principally brings highly dispersed, information-driven 'customer' organisations together to help to resolve specific issues they face. Such organisations may be individual entities, or multiple collaborating or trading entities ('virtual organisations'). Individual entities include global-scale corporations; national and regional institutions in both the public and private sectors; and local concerns, including small businesses. The common need is to participate in collaboration and commerce over open networks.

Large organisations will inevitably form an important part of Jericho Forum's constituency since they face the issues within its scope most acutely, and have the skills and resources to address them and influence vendors. However, Jericho Forum's approach – to drive out principles and standards – will benefit smaller organisations and individuals, once the principles and standards have been developed and adopted widely. Small organisations and individuals will have a role in ensuring that Jericho Forum principles and standards do not impose undue costs on them, and that standards-conformant solutions are usable regardless of organisation size or structure.

Jericho Forum also brings together academia, and individuals who need to participate in collaboration and commerce over open networks and need to play a role in shaping security processes, services, and standards. This includes the 'open source' community, many of whom work outside 'organisations'. These individuals offer a rich knowledge base of what works, may work and does not work. They can often demonstrate crucial insights on security problems and the ability to devise innovative solutions.

Role of vendors

While Jericho Forum exists principally for 'customer' (or 'end-user') organisations and individuals, it recognises the need to involve vendors. They will be able to participate fully in Jericho Forum Working Groups and via the Vendor Advisory Council, as discussed further in section 4.

Other standards bodies

Jericho Forum will aim to work with other standards bodies and forums to evolve current standards or define new ones, if they need better alignment to satisfy Jericho Forum's business drivers and principles. It will therefore develop principles and standards collaboratively, not in isolation. It recognises that vendors and service providers will create the solutions that will underpin Jericho Forum's vision, and other standards bodies may develop detailed requirements for particular topics and subject areas.

2.4 *Jericho Forum's Scope*

Jericho Forum exists to develop principles and standards for secure collaboration and commerce over open networks. The security issues of concern have two common themes:

- They are ICT related (rather than purely business related)
- They span organisational and ICT domains and boundaries (rather than issues centred on individual domains under the sole control of individual organisations).

Jericho Forum will therefore focus primarily on information flows that span organisations and individuals and how to secure and manage these across open networks. The focus will be on business to business (B2B) and business to government (B2G) flows, but not exclusively. It will take into account information flows involving for example employees, customers and the general public.

Jericho Forum will consider all aspects of security: confidentiality, integrity, and availability (some authorities treat communications security issues such as non-repudiation and privacy related issues such as anonymity as additional aspects of security; all are in scope). It will focus on business drivers as well as security topics and work collaboratively to address detailed technical requirements for these topics. It will take the vendor market, regulations, and economic factors into account.

The issues of concern are discussed further below.

2.4.1 *Business and economic issues Jericho Forum will aim to address*

Formulating the business case for security

There are many potential opportunities and threats that improved information security can address. The business case for better security within and between organisations may include enabling agility/flexibility, cost reduction, productivity, integrity and reliability; greater value derived from increased collaboration and commerce, risk management, simplification, usability, and enhanced reputation/brand value.

There are mutual dependencies between de-perimeterisation and each of these factors. When multiple organisations or individuals collaborate, they may share risks and revenues, leading to a need for common business cases and an equitable distribution of security costs.

Formulating and understanding security goals and requirements

Standardising the ways security goals and requirements are communicated is difficult. Many underlying goals (why and what security is needed) remain tacit within organisations, and requirements end up being articulated as specifications of the security controls baseline (how security will be achieved) without a clear rationale.

So long as security controls are solely the concern of the organisation, this is of no fundamental concern. However, Jericho Forum considers that as more organisations are involved in collaboration and commerce, articulating security goals and requirements consistently, based on an accurate view of existing security capabilities, and using standard languages, becomes much more important. De-perimeterisation will be difficult to achieve if the organisations involved cannot agree: why security is necessary; the scope it should cover and what each organisation

expects it to achieve. It will be difficult to manage if failures to achieve agreed security levels are difficult to detect and enforce.

Privacy and security for all forms of collaboration and commerce

As discussed above, securing B2B/B2G collaboration and commerce over open networks is one of the main themes for Jericho Forum. However, many Jericho Forum members deal with individual consumers, employees and members of the public (business to consumer, B2C, business to employee, B2E, government to public, G2P or business to public B2P) over the same open networks as they want to use for B2B/B2G collaboration and commerce. They seek common standards and solutions to underpin the privacy and security of these various information flows.

Jericho Forum also recognises that part of the challenge many organisations face in exploiting the potential for ICT to support B2B, B2C, B2E and B2P is that consumers, employees and the public need to gain confidence that an organisation will protect their security and privacy. Their information may flow within the organisations, and to other organisations.

In the context of individuals collaborating over open networks, so-called Peer-to-Peer (P2P) information flows are also relevant, and P2P technology provides a potential source of innovation and solutions, as well as a threat when it bypasses organisational controls. Jericho Forum recognises its relevance and also the challenges it poses in balancing individual, organisational, and societal rights and responsibilities (e.g. the abuse of P2P technology by criminals).

Jericho Forum will support, and act as an advocate for, the responsible, private and secure exploitation of ICT for consumer and other private data, and for other information over which individuals and organisations have legitimate contractual, moral and legal rights.

Offshoring and outsourcing

Increasingly, collaboration and commerce involve external access to an organisation's ICT infrastructure (databases, applications, networks and systems) and information. A critical business challenge and constraint is to facilitate cost savings and efficiency gains through outsourcing and offshoring infrastructure and business processes while upholding privacy and security. Principles and standards must also be sufficiently flexible to support outsourcing, subcontracting and offshoring to individuals (i.e. sole traders working from home offices).

Technology cost reduction

Achieving required levels of protection and security management simply and cheaply is always a critical business challenge, even more as access and interoperability requirements increase.

Organisations find that their current infrastructure was not designed with such increased requirements in mind. Security controls can be complex and inflexible when they need to protect multiple dissimilar access paths, methods and protocols. Organisations' networks and the firewalls at their security perimeters may need to be redesigned to reduce overall costs, and improve usability, responsiveness and flexibility. Redesign will be more difficult if ICT products and solutions require construction from scratch.

Jericho Forum sees the need for standards to drive out common solutions from vendors, available off-the-shelf, thus reducing costs. It also sees the potential dangers of over-engineered 'standards' that simply seek to codify inappropriate designs and interfaces.

Organisation-specific business issues and drivers

Jericho Forum will link the principles and standards it develops clearly to business drivers and benefits. Understanding security controls effectiveness and the ability to justify these to regulators and other external stakeholders are inherently difficult business issues confronting the security community as a whole, through developments such as:

- The Basel II Accord affecting the global Financial Services industry
- In the US, laws with direct implications on handling data about individuals and safeguarding its security when passed between organisations. For example: the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Biley Act (GLBA).

2.4.2 *Security issues Jericho Forum will aim to address*

Risks and requirements

The information involved in collaboration and commerce over open networks may:

- Represent sensitive know-how, private or personal information, so require protection against unauthorised copying or disclosure;
- Have stringent integrity or availability attributes, in support of critical business processes or electronic commerce, so require robust and reliable communication methods and clear accountability for exchange between communicating parties; or
- Represent the internal operating parameters for technology infrastructure or business processes (for example, when an organisation's infrastructure or process administration is outsourced to an offshore service provider).

Protection may be required both when information is at rest and in transit. Some or all of these requirements may apply; so working out how to identify and manage security risks for an organisation's particular circumstances and thus select appropriate and cost effective technology is critical.

One size does not fit all

When multiple business entities and service providers are involved in collaboration and commerce, agreeing what risks apply and so which controls are needed, is even more critical. Security requirements and standards of large organisations may be difficult to apply to smaller organisations that interoperate with them. Security that is simple and cheap to deploy but does not meet the most stringent requirements may none the less mitigate risks sufficiently in many cases.

Existing perimeters and security controls

Firewalls and proxies have protected the security perimeters between internal (closed) and public (open) networks for many years.

When access requirements between networks are simple, and the protocols involved are equally simple, a firewall is simple to design and operate, and if properly managed provides good network security. Proxies at the firewall provide filtered or encrypted communication to counter threats to data in transit or exclude unwanted data and access.

However, for complex networks, protocols and application access requirements involving customers, business partners or suppliers, firewall complexity and cost of operation will rise. There will be an increasingly complex relationship between security controls at the firewall/proxy and those at internal end-systems and applications.

Many communication protocols now run within the web (HTTP) protocol to allow 'tunnelling'; indeed arbitrary tunnelling is possible rendering 'layered' communications architectures meaningless. Increasing proxy complexity will result in decreased performance and increased cost and management complexity.

De-perimeterisation involves re-appraising where security controls are positioned, re-balancing cost and complexity. This may involve moving security controls from firewalls or proxies to internal end systems or applications, or if the confidentiality or integrity of data is paramount, to move controls from the systems and data repositories that hold data at rest to the data itself (i.e. using cryptographic techniques).

It will involve careful appraisal of the methods by which security controls (whether positioned within communicating endpoints or within the protocols they use to communicate) are themselves controlled or managed, and the potential for this control and management 'plane' to be disrupted, subverted or defeated.

For example, when communication protocols freely mix control/management information and the data representing business information within protocol messages, the strict separation that these different types of information enjoy within the host systems/endpoints will break down, leading to heightened risk of loss of availability and integrity. Traditional assumptions that, for example, certain protocol port numbers are 'reserved' or 'privileged' (thus inaccessible to arbitrary hostile communicating applications) are unenforceable in a de-perimeterised scenario.

Over time, new security controls and boundaries will therefore need to be consolidated and maintained in order to uphold confidence and realise continuing benefits (this enduring process can be considered to be ***re-perimeterisation***)

Current and future technology issues

Jericho Forum will address both long-term technology evolution (i.e. over the three to five year periods which vendor product roadmaps typically envisage) and short-term tactical requirements for de-perimeterisation. Security technology topics will include, where relevant:

- Authentication and access control
- Next generation Internet protocols
- Encryption, PKI and key management
- Policy management
- Automated data and information classification and management
- Identity management

- Intrusion detection and prevention
- Information flow content scanning.

Monitoring, incident handling and management

Centralised monitoring, incident handling and management of ever more complex security controls also becomes increasingly challenging as organisations, their technology, users and information disperse across global open networks; access requirements increase; and relationships with customers, suppliers and business partners become more interconnected. When multiple business entities are involved, maintaining a single centralised controls management system will become impossible.

Incident handling (and supporting technologies such as intrusion detection/prevention), which detects and mitigates risks that occur, can be frustrated by preventative security controls. For example, network intrusion detection needs to scan network traffic, but if this is encrypted and the intrusion detector cannot decrypt it, the detector will be blind.

Experience shows that monitoring, incident handling and management capabilities must be inherent in any security design, and are difficult or impossible to retrofit without breaking other security controls or non-security functionality. De-perimeterisation must overcome this risk.

Interoperability

Interoperability will be central to achieving Jericho Forum's mission. Interoperability requires open interfaces, as well as compatible architectures behind the interfaces to ensure the semantics of each interface are tractable, and that interfaces can be combined and composed without unintended consequences for security.

Emerging approaches to repackage existing technology interfaces and information flows (i.e. using 'web services') can provide partial interoperability. However, these approaches fail to address all collaboration and commerce requirements, and need to 'bolt onto' a huge variety of existing technology of variable quality, which could increase costs and decrease performance.

Interoperability can therefore conflict with appropriate security. Organisations need to position security controls optimally for each information flow, and integrate them with internal security controls, rather than bolt them on for the sake of appearance.

Security controls need to coexist with commercial off the shelf (COTS) products and solutions (especially operating systems) whose architecture and design may also reflect arbitrary historical security decisions that do not translate well in the de-perimeterised world. In the absence of freedom to redesign COTS technology or re-implement its (non-security) functionality from scratch, organisations will want to live with its vulnerabilities, trading off security with risk and cost reduction. (Here COTS includes open source software which may be acquired and deployed on a non-commercial basis.)

In this situation security design goals focus on recoverability, assuming the scenario where the COTS technology is attacked, fails, gets patched to remove the vulnerability, and needs to be redeployed in a 'known good' (or 'known good enough') state. Similar considerations apply to data, or at least to working copies of data which can be recovered from 'known good' masters.

Finally, new infrastructure standards that are being developed (for example, grid computing) can magnify existing security cost and performance overheads, thus impeding the achievement of the potential business synergies and efficiencies, for example via greater collaboration in the supply chain or across distribution channels, that those standards are intended to facilitate. De-perimeterisation must ensure such developments and risks are taken into account.

Assurance and trustworthiness

Assurance of the reliability and integrity of organisations and their ICT can increase in many ways, including by using evaluation, certification and inspection, and agreeing or imposing common standards and solutions. Many organisations use these approaches as a prerequisite to on-line collaboration and commerce with other organisations, and to determine the level of trust they need to develop with other organisations.

Certifiability and evaluatability are therefore important, but do not enjoy universal appeal due to their significant overhead, leading to undesirable outcomes such as inability to patch or upgrade technology cost effectively without invalidating the evaluation/certification. In general, attaining high levels or degrees of evaluation/certification critically depends on design simplicity and tractability. A software product comprising millions of lines of code with un-countably more potential execution paths, modes of operation and behaviour is fundamentally un-evaluatable in the full sense of the term. A more limited goal focusing on continuous testing may provide equivalent trustworthiness with lower impact.

In an operational security context, an ability to determine the relative level or degree of trustworthiness continuously and in real time will be more useful (either as an alternative to assurance based on evaluation/certification or as a complement to it, depending on the nature and value of the business relationships involved). This may be part of management and monitoring at an organisational level, or may be a direct end user requirement, for example the ability to distinguish whether a remote web site is genuine or 'spoofed', or the ability to verify the degree of protection available at a collaborating partner by means of records of controls initiation and operation.

De-perimeterisation must support these requirements.

2.5 *What is Out of Scope?*

Jericho Forum will not seek to develop technology, general-purpose security standards, guidance or advice to cater for the broad security and business concerns that organisations have to face individually. These include: monitoring employee behaviour, filtering 'spam' email, educating and training end-users to follow internal security policies and standards, hardening COTS IT platforms against malicious attack, organising and staffing security teams, vulnerability testing, and estimating and tracking broad security costs and benefits (beyond those associated with securing collaboration and commerce).

Jericho Forum does not seek to resolve wider issues of technology interoperability that do not impinge upon security, but will consider them appropriately. It has a vested interest in the standardisation of, for example, information representation, data access methods, outsourced service delivery and distributed ICT infrastructure management, because common standards in these areas imply corresponding common security standards.

Balancing this, Jericho Forum needs to address a wide variety of organisations' and individuals' situations, including existing investments in ICT that use multiple overlapping, obsolete and conflicting technology that cannot be replaced easily. In these situations, organisations will need several options to meet their goals for collaboration and commerce (depending on the appetite for change, speed and cost factors), including evolutionary technology upgrades, purchase of additional integration technology, and contracting out interoperability to service providers.

Jericho Forum will liaise with general technology standards groups such as the Open Group that seek to tackle wider issues of interoperability, acquisition and adoption options, and technology evolution.

3 Moving to a 'Jericho World'

3.1 *Introduction*

For an organisation to move to a 'Jericho World', it will typically want to improve collaboration and commerce in one or more of the following ways, in increasing order of difficulty:

- Provide low cost secure wide area network connectivity supporting a variety of geographically dispersed business units, with facilities of different kinds
- Support personnel involved in critical business processes who are mobile or work from home or other premises the organisation does not control; they may roam inside and outside the organisation (e.g. use a laptop computer to connect to systems, applications, and information services, both internal and external to the organisation)
- Allow access by and partnerships with outsourced service providers, customers, sales agents/distributors and/or suppliers involving the organisation's systems, applications and internal data
- Improve flexibility to allow the shape of the organisation and its business relationships to change dynamically.

3.2 *Application context for de-perimeterisation*

Collaboration and commerce involve application tools and capabilities such as:

- Portals – supporting controlled sharing of information and access to applications via common presentation and data formats
- Calendaring, conferencing and messaging – supporting e-mail, discussion groups etc.
- Workflow – supporting scheduling of collaborative business activities (e.g. supply and distribution chains), validation and approval processes etc.
- Analysis and forecasting – supporting fusion of performance data both quantitative and qualitative, from multiple internal and external sources
- Marketplaces and auctions – supporting buyer/seller discovery and procurement activities
- Knowledge management systems – supporting intellectual property development, learning and training
- Pricing, execution, delivery and settlement – supporting trading.

De-perimeterisation may affect any of these tools and capabilities. They may be stand-alone applications, linked together, or contained within larger applications/systems (e.g. Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM) systems). There may be links to other applications, for example, where workflow tools link to computer aided design tools to support collaborative engineering design.

3.3 *Architectural context*

Constituent parts of applications/systems may be integral to that application/system, or shared, as in the situation where enterprise architecture implements common components and ICT infrastructure used by multiple applications/systems. These parts are:

- Process – the dynamic component of each tool or capability, or overarching business operation (process logic – the ordering and sequencing of process steps)
- Business Logic – the constraints and rules (including security) that must be upheld to meet business objectives; these may be embedded in applications, or implemented by other architectural components
- Data – both the underlying data itself, and data descriptions (meta-data) that support data communication and sharing
- ICT Infrastructure – further discussed below.

De-perimeterisation potentially involves positioning or re-positioning security controls in any of these parts. Especially, within infrastructure there may be network security controls that de-perimeterisation repositions to host computers or other devices. The potentially affected areas are:

- Local security components (edge controls – firewalls, routers, intrusion monitoring (but see section 2.5) – and secure communications)
- Platforms/devices (middleware and messaging systems, database management systems, host computer operating systems, embedded operating systems)
- Interface standards (communications, data, security)
- Management frameworks (policy, identity and access, audit, incident and vulnerability)

As discussed in section 2, the established architectural notion of 'layering' while providing a conceptual aid to analysis of existing security controls and design of new ones is increasingly less useful for security once considerations such as tunnelling are brought into play.

3.4 *Business scenarios – overview*

The remainder of section 3 illustrates de-perimeterisation via a number of business scenarios grouped into the categories introduced above as ways in which organisations want to adopt de-perimeterisation:

- Provide low-cost secure connectivity
- Support roaming personnel
- Allow external access
- Improve flexibility

Each scenario notes whether the business and technology issues it exposes are short term, requiring tactical solutions, or long term, requiring the development of fundamental standards and their adoption by vendors.

The business scenarios presented here are in outline form; the goal being to illustrate relevance and value and to help gain buy-in, rather than specify requirements completely. A fully specified scenario would include the definition of business processes or application(s), underlying business and technology environments, actors involved, and the goals and outcomes that stakeholders in the scenario expect. Jericho Forum's Working Groups will develop each scenario outline further, as required to underpin their work.

3.5 *Provide low-cost secure connectivity*

3.5.1 *Access over wireless and public networks*

Context

- Organisations wish to use public and private wireless (IEEE 802.11 standards based) networks to open up access to internal systems, data and applications. The path of access may be via an Internet access point at home, or in a hotel, or via wireless networks and service providers at, for example, airports and customer/ business partner sites. Web based applications may also be deployed for public access at Internet cafés and similar facilities.
- Many organisations have opened up external access to internal applications protected by existing authentication protocols/mechanisms, reckoning that security risks to these mechanisms are not significantly increased. Often it is assumed that the 'secure pipes' provided by Secure Sockets Layer (SSL) and Virtual Private Networks (VPN) provide sufficient extra protection.

Issues

- Using public web access facilities and wireless networks renders authentication protocols and data more vulnerable to interception, 'spoofing' and 'man in the middle' attacks. If a protocol binds a communicating endpoint to its domain name and the naming service is vulnerable to attack (e.g. masked from within the local wireless bearer network) then the binding can be tempered with. If the user's browser contains (or the user can be tricked into downloading) invalid root digital certificates which nevertheless validate a web site certificate with an apparently correct domain name, an attacker can impersonate an apparently certified web site.
- An underlying problem is that surfing the web involves applying an at best only approximately articulated end user security policy regarding which sites he or she wants to visit under what circumstances. The capability of browsers to categorize sites as 'trusted' or corresponding to various 'zones' is not sufficiently granular from an access control perspective, and too abstract from the viewpoint of end-user comprehension.
- Most simply, if a spoof web site certificate is simply invalid and the browser does issue an error message, the end user may override this message anyway.
- Similarly, communications paths involve a patchwork of technologies with non-integrated security protocols, so complexity and incomplete security capability will result. Side effects such as wireless routers/bridges crashing when virtual private networking (VPN) is enabled are common. Device configuration is difficult. The user reaction is to leave factory default settings untouched and/or disable the offending security technology.

- Web browsers and their underlying operating environments often provide a permissive environment for unwitting execution of web content. Any user dialogue or protocol required for initialisation/establishment of trust relationships is open to subversion of the end point operating and browser software.

Ease of resolution

- Interoperability and integration of wireless security technologies are short-term issues, but end point and wireless device technology originally built with minimal attention to security needs to evolve in the long-term.
- Common problems are a lack of security-positive design (ensuring better visibility of security assumptions to the end user, and removing default insecure behaviour), and the weak trust model inherent in publicly available public key infrastructure (PKI) hierarchies used to bind computers/devices/their users to logical identifiers such as domain names or IP addresses.
- Deploying stronger authentication protocols with anti-replay controls (e.g. challenge/response, cryptographic techniques based on Needham-Schroeder principles) may be feasible but may not scale sufficiently for de-perimeterised scenarios (critical requirements may include a common time source, and frequent re-authentication, which will impose overheads)
- Jericho Forum will maintain an overview of practical issues organisations encounter in this area, determine shortcomings in existing standards and their implementation, and work together with relevant standards bodies to resolve them. It will examine how 802.1x standards can evolve and integrate better with other infrastructure elements.
- For the long term, Jericho Forum will promote integrating and managing information about the identity of the individual, the device and the location independent of the data transfer technique.

3.5.2 *Domain inter-working via open networks*

Context

- TCP/IP supports the design of resilient networks. Organisations can add and remove devices and parts of the network while the remainder continues functioning. Modern routing and switching capabilities enable organisations to maximise network bandwidth utilisation, adapt networks to new communication and service requirements, and optimise performance.
- Network architecture can contribute to security by dividing an organisation's networks into a number of security domains – typically implemented by segregating sub-networks using routers and internal firewalls, and filtering network traffic by service and/or source/destination addresses, or requiring additional user authentication to the network domain.
- Address configuration can be static, dynamic or a mixture, but typically limited to an individual network domain. Current (IP version 4) network technology does not support managing multiple classes or qualities of service within the same topology.

- Organisations typically provide dedicated sub-networks and/or use switched (layer 3) networks (virtual LANs) to reserve bandwidth for particular users, services or applications. Multi-protocol label switching (MPLS, a layer 2 technology) can provide insulation and separation between the communications paths assigned to different subscriber groups/services.
- In a disaster scenario, an organisation facing significant risks from loss of physical facilities will typically wish to revert to a standby infrastructure. In order to reduce the standing costs to maintain this infrastructure, it may be desirable to provide less than full service, capacity and performance, sufficient only for essential business operations during the temporary duration of the DR scenario.
- This is increasingly a standard business requirement. The market for computing power and other information processing resources as openly tradeable commodities is starting to develop. Ideally, organisations should be able to provision infrastructure and services flexibly, on demand and at very short notice, depending on the level of business operations that need recovery using the standby infrastructure.

Issues

- Many organisations will approach de-perimeterisation 'from the ground up', which is the core issue in this scenario. De-perimeterisation needs to take into account the security domains, flexibility, and performance that private networks aim to deliver currently. If an organisation replaces a single global network domain (interconnected organisation-wide WAN) with open networks, the organisation needs to ensure that qualities of service, robustness and resiliency continue, traffic segregation is achievable, and that it can change requirements for these 'on demand'.
- The practical impacts of interposing domain boundaries can be severe. For example, encrypted tunnels (SSL or VPN) may be hardwired to domain names and IP addresses which therefore cannot be changed without reconfiguration. Secure access at the level of a VPN has little granularity and opens up risks of access rights abuse and privilege escalation. In many cases only limited and selective access is needed.
- The economy of scale benefits of outsourcing to shared infrastructure managed by an infrastructure service provider will be reduced if the provider has to physically implement multiple segregated mini-domains to match the outsourcing organisation's domain structure.
- An organisation may accept degradation of qualities of service, robustness and resilience from de-perimeterisation if this reduces costs significantly. However, to do so will limit de-perimeterisation opportunities to undemanding users and applications.
- As voice and data services converge, organisations increasingly need to be able to manage bandwidth dynamically and on demand, and rapidly provision both end-user devices and supporting infrastructure/services. De-perimeterisation requires that open networks should replace private networks to reduce costs, but this approach is hampered if organisations cannot manage bandwidth and qualities of service provision consistently within an open network environment.
- Layer 2/3 switching (Virtual LANs) provides simple network traffic segregation for the purpose of bandwidth management and containing the impact of rogue broadcasts but this is inflexible, has broadcast mode as its failure condition (thus removing the segregation) and is not designed to resist attack (the tagging used to segregate traffic can easily be forged).

- MPLS is more secure but is complex to implement and not contemplated outside backbone service providers.
- Infrastructure control and management protocols suffer from a history of insecurity and piecemeal evolution. Whilst extensible authentication protocols (e.g. Diameter) have been specified more recently, implementation support varies and any extensible schemes are prone to incompatible vendor extensions.
- Using open networks as backbones requires reconfiguration of naming and addressing, and network address translation (NAT) and/or protocol tunnelling to allow multiple communicating domains to interoperate. Additional infrastructure and protocol sophistication (e.g. Mobile IP) can reduce this impact, but at additional cost and complexity.
- Fault finding and troubleshooting requires visibility of sub-network and router status across the end-to-end communications path so that fault resolvers can examine each hop in the path. Typically, organisations and service providers have to construct status monitoring and troubleshooting capabilities from scratch, as there is no standard approach.

Ease of resolution

- These are short and long-term issues. Non-interoperability of proprietary extensions for extensible management and authentication protocols requires immediate focus.
- IPSec standards are starting to mature, but are complex and only implemented at a premium cost at present. IP Version 6 addresses many of the quality of service and performance requirements discussed above, and implementations in mainstream platforms are starting to appear. However, the need to interwork IPv6 implementations across the extant IPv4 Internet has led to considerable design complexity.
- The IETF has developed draft mobile IP standards for both IP version 4 and version 6 to enable organisations to attach fixed sub- network addresses to open networks without reconfiguring the address space, but these are yet to achieve widespread use. It is likely that only IPv6 based mobile IP will gain significant momentum.
- Service monitoring and management standards that can support controlled information sharing are not yet under development. Jericho Forum will need to provide a lead here.
- Jericho Forum will further analyse the practical network security, service provisioning and management issues organisations face in moving to an open network model, and establish liaison with the IETF and other working groups working in this area. It will act as an advocate to pool demand for IPSec support and enhanced service management capabilities from service providers and vendors.

3.6 *Support roaming personnel*

3.6.1 *Phoning home from a hostile environment*

Context

- Roaming personnel wish to log into the organisation's intranet to access internal applications and information from a customer's IT system or other 'foreign' remote computers. This supports various business situations such as sales force checking product availability and pricing while at a customer's premises.

Issues

- Typically, organisations that need to provide this type of capability for the sales force or other mobile workers and feel there is a significant risk, do so by providing cut down versions of the full applications or information, delivered over the web or mobile data services. This can be inflexible, costly and awkward to use. A mobile workforce may increasingly demand full functionality and information access regardless of location.
- Provided an organisation delivers all applications and information for external access over the web, using SSL and strong authentication can address most authentication, access and communications confidentiality and integrity issues in this scenario. However, the protocol design assumption is that binding secure communications to endpoints denoted by IP addresses or domain names is acceptable, and in addition end to end key management generally assumes manual key distribution as a foundation of trust in the keys (ultimately, even for self-signed root public key certificates, taking a strict view of 'trust'). As already noted, secure pipes cannot protect data once delivered and decrypted to a 'hostile' host system.
- In many environments, there is no permission for encrypted traffic to traverse internal networks, so mobile visiting personnel who want to connect to their home organisation must rely on dialup or limited coverage wireless access via service providers and public networks.

Ease of resolution

- The availability of communication paths that can be secured using point to point security protocols is a short-term issue. Increased availability of mobile wireless data services and voice/data convergence in most industrialised countries will allow organisations to reach their mobile workforces directly and at low cost.
- Identification and access management for roaming external access back to the 'home' organisation, partly through technology, partly through process, can limit access to authorised ways. However, extending the scenario to take into account the possibility that an individual does not use an organisation's 'owned' device/platform, so that the organisation cannot trust the device being used to attack the data or systems it is used to access, breaks the trust assumptions underlying the use of existing remote access techniques.
- Jericho Forum will monitor standards developments in this area and consider further the practical issues organisations face in adopting them.

3.6.2 *Enable portability of identities and data*

Context

- Secure data portability may be desirable in some situations. This includes the ability to use a home computer, the corporate laptop or other arbitrary computers to work on sensitive data, with easy transfer and backup of information to the 'home' organisational server.
- Roaming personnel may require portability of authentication credentials, potentially including cryptographic keys, biometric data, passwords and other relevant information. This enables use of Internet cafés and other public IT facilities, relying on a phone/ personal digital assistant (PDA) for high priority messages and data, therefore reducing the need to carry a larger portable computer.

- By extension, the ability of an individual to establish a 'known good' processing environment on a public or otherwise non-owned device would provide further assurance that the secure data is being processed in an acceptable manner.

Issues

- The three areas discussed above are interrelated. De-perimeterisation requires an organisation to re-appraise the implied trust relationships between an individual, the individual's 'own' data set, and the host systems, data containers, and network security domains that currently authenticate the individual, and protect the data.
- If data is to be portable outside existing protected containers and security domains, organisations must deploy encryption capabilities. Data security then becomes dependent on the security of keys and the devices or mechanisms that manipulate them.
- Existing key management techniques are largely manual and difficult to scale, especially for symmetric keys. Cryptographic key management must allow for alternate authorised access (e.g. an executive and the executive's personal assistant), controlled information sharing among groups, and protection of key material in case of loss or theft of the device or token that carries it. It must be possible to apply further granularity to key provisioning and usage, not relying on the essentially open-ended and unenforceable attributes defined for public-key certificates.
- Much of the foundation work occurred without clear business requirements in mind or buy-in from end-users. The X.509 standard leaves the majority of implementation concerns (even at an architectural level) under-specified. PKIX and related standards attempted to add architecture and management for multiple applications into the X.500/X.509 model. Unfortunately X.500 directories were largely non-existent before PKI came along; the naming conventions proved to be awkward to map to existing schemes and inflexible for multi-organisational use; and the revocation model proved to be unsuitable for many deployment scenarios.
- The result was extensive development of revocation management, certificate extensions and other functionality to address specific business requirements. Inevitably vendor dependencies and proprietary extensions crept in. The cost and complexity of implementation in turn served as a barrier to the emergence of PKI-aware applications.
- In addition, organisations have found it difficult to apply the 'trusted third party' model in PKI to real business requirements. If a third party issues a logical 'identity', it is potentially liable for mis-issuing it, or compromising authentication credentials with which it is associated (depending on the credentials and the mode of issue). Framing a contract that can encapsulate this, while providing equitable commercial incentives for both service provider and subscriber, has proven to be very difficult.

Ease of resolution

- This is mainly a long-term issue. The fact there is a long history of standards development and a relative lack of standards adoption suggests that it will be difficult to resolve without redesigning existing PKIs. Simple approaches to deploying limited-use PKIs have been proposed and can serve as a 'quick fix', but may not suit the de-perimeterised world.
- Some aspects of PKI standardisation and deployment lessons that have been learned should not be ignored. As new XML based protocols and standards appear there is a risk is that old protocol and implementation bugs will reappear.

- Jericho Forum will re-consider, at a fundamental level, the trust relationships and usability issues involved in cryptographically-secured collaboration and commerce for a variety of business scenarios, and then appraise the suitability of existing key and certificate management approaches to underpin these relationships. There will need to be a particular focus on key management.

3.7 *Allow external access*

3.7.1 *Application access by suppliers, distribution agents or business partners*

Context

- Major applications support critical business processes including sourcing, production scheduling, selling, and purchasing. As originally designed, the applications help internal users within the organisation carry out these activities, with separate IT or paper interfaces to the external organisations involved.
- Competitive or other pressures on the organisation increasingly require granting suppliers, distribution agents and other business partners direct access to internal applications, e.g. so they can see inventory records to determine supply delivery schedules. Direct access can speed up the overall business process, eliminate the need for internal users to act as interfaces, and offer other synergies and benefits.

Issues

- Passwords securing existing access to systems and applications will be inadequate to control access from the outside, being vulnerable to various types of malicious software attack.
- The vendors of proprietary supply chain applications (e.g. ERP) may offer various options to support remote access including linking to web portals or direct support for remote sign-on. Unless the standards these options support are fully documented and validated, security managers may have significant concerns about implementing them (for example, undocumented use of insecure client/server protocols that provide loopholes that viruses and hackers can exploit).
- Full access to internal applications and information may only be deliverable over a VPN connection, but this implies a long-term remote access capability. If a VPN is used from a potentially 'hostile' machine there is no way to limit how network access is regulated, which means installing intrusion monitoring to watch remote access and shutting the connection down if unauthorised activity occurs.

Ease of resolution

- This is a short-term issue. Jericho Forum can bring together customer organisations that depend on large scale ERP and CRM applications, and pool demand for greater flexibility of external access solutions, conformance to standards, and interoperability.
- Jericho Forum will examine how VPN standards can evolve to facilitate limiting onward access rights and terminating VPN tunnels at specific internal network addresses.
- There is a limit to the extent that Jericho Forum can resolve current issues. 'Legacy' applications and systems that grant excessive privileges to users need to be replaced or reworked to provide finer grained control of privileges and access rights.

3.7.2 *Outsourced help desk access to internal systems*

Context

- Help desk and IT support teams need privileged access to an organisation's applications and systems in order to diagnose problems, administer access and perform routine housekeeping. Increasingly, service providers outsource these roles, even if the overall ICT infrastructure and applications remain in-house.

Issues

- Many organisations lack single sign-on capabilities of sufficient strength that can unify privileged access to systems and applications. There may be dozens or hundreds of systems and applications in a large organisation, each using its own sign-on method. The internal debate often centres on the need for a 'strategic' solution for single sign-on, but the help desk requirement by itself cannot provide a sufficient business case to adopt such a solution.
- Granting privileges concentrates the risks associated with the people and user accounts concerned. In addition, the privileges involved may allow access to data and functionality in excess of that strictly required for the help desk or support team's duties.
- There are long standing issues in many systems regarding excessive privileges. Risks associated with excess privileges are containable when the people to whom they are granted are in-house, but outsourcing may weaken the ability to compensate for these technology risks by additional procedural and personnel security controls. One paradox of implementing single sign on for administrators is that the potential impact of insider attack and access rights / privilege abuse will be far greater.

Ease of resolution

- This is a short-term issue with long-term aspects. There are several proprietary technology options, including password synchronisation and single sign-on that avoid the need to re-engineer existing systems and applications to use a replacement sign-on mechanism. These are viable for many organisations in the short-term. However, while they may mitigate risks emanating from the underlying communications medium, they do not address the risks that the administrators' increased power to affect multiple systems will not be abused.
- The long-term 'strategic' solution that has emerged so far involves 'federated' identities and authentication standards, but these require customer organisations to agree that the trust models underpinning the standards are suitable, and vendors and service providers to agree on and demonstrate interoperability.
- In addition, monitoring, incident handling, dual control, and other additional security issues will need to be addressed from the definition of the trust model onwards, in order to address the risk of insider attack. Jericho Forum can play a role in identifying the gaps, and pooling requirements to build demand with vendors to resolve interoperability.

3.8 *Improve flexibility*

3.8.1 *Connect Organisations for EDI Using Secure XML Messaging and Web Services*

Context

- Many organisations have initiatives underway to redesign systems and interfaces to use Extensible Markup Language (XML) and so called 'Service-Oriented Architectures' (SOA). For example, healthcare organisations have revised the HL7 messaging standards to use XML. Organisations are starting to deploy XML now that mainstream off the shelf software has XML built in. XML standards are vendor independent, so organisations hope that their adoption will facilitate interoperability and greater vendor competition hence reducing costs.
- The World Wide Web Consortium (W3C), supported by other standards bodies, includes a number of security standards within the XML standards set: Encryption, Digital Signatures, and Key Management.
- Higher-level 'trust' standards concerned with identity and access management (e.g. Security Assertions Markup Language (SAML)) are also under development. W3C's SOAP (Simple Object Access Protocol) and related standards for Web Services have spawned standards such as WS-Security to provide services (data integrity, confidentiality and authentication) for message based communications security.
- Achieving security interoperability for an end-to-end information flow between two applications in different organisations, crossing multiple security domain boundaries, requires three things:
  - a suitable authentication context for the information flow (potentially provided by the token formats defined by WS-Security)
  - security attributes are associated with the information flow (potentially provided by SAML)
  - communicating applications/systems maintain the security session context across multiple message exchanges and domain boundaries for the information flow.

Issues

- Using underlying communications protocols to implement the session context relies on either weakly secure mechanisms e.g. encrypted cookies, or transport layer security (e.g. SSL based). An organisation's internal applications and systems typically rely on security mechanisms in the host platform/system environment. These in turn use proprietary and non-interoperable logical 'tokens' to communicate identity, security attribute and session context information.
- Mapping existing security attributes such as the user-IDs and group memberships of local operating system environments or authentication frameworks between different security domains is cumbersome and will not scale. Passing information across domain boundaries may involve dissimilar transport and cryptographic key management protocols whose security mechanisms do not interoperate (e.g. SSL and SSH).

- Vendors favour a slow evolution towards standards-based end-to-end security using SAML and WS-Security, and encourage customers to adopt their existing products for initial single-domain implementations. There is no point in doing this if multi-domain operation will require starting again from scratch.
- There is a potential of a conflict of interest, or at least divergence of vendor interests. Vendors have to provide increasing compatibility with both prior proprietary standards and emerging vendor neutral ones, simultaneously trying to keep solutions sufficiently simple to be trustworthy. Costs increase.
- Although vendors may profess a willingness to adopt neutral standards, prior efforts to achieve network security interoperability for Kerberos-based authentication frameworks do not give confidence that vendors will resolve this issue easily. There is a risk that overly complex and inflexible perimeter security controls will re-emerge.
- Web services security depends on underlying assumptions of trust in existing authentication frameworks. The standards need to cater for organisations that want to leverage their PKIs, Kerberos systems etc. If these assumptions are incompletely addressed (or not at all), the foundation collapses. As PKI has had limited success in enabling inter-organisational collaboration and commerce, there is a risk that XML security will perpetuate potentially unsuitable underlying security frameworks.

Ease of resolution

- This is a long-term issue although suitable existing standards initiatives are underway. Web Services are flexible and extensible, so in principle can support de-perimeterisation. However, this very flexibility has bred complexity. At a fundamental level, communications security services must depend on cryptographic techniques, which are easy to implement insecurely (or difficult to implement securely, depending on one's viewpoint).
- Jericho Forum will aim to overcome the potential hindrances discussed above by developing end-to-end identity management, authentication and trust models, with supporting key management architectures, so that organisations are better equipped to leverage existing frameworks without being tied to their original design assumptions.

3.8.2 *Consolidate identity and access management (IAM) systems for collaboration and commerce*

Context

- Identity and Access Management (IAM) refers to a class of security functionality and systems concerning the unified management of user authentication, authorisation, and access to data and systems. Although IAM may apply narrowly to password synchronisation and single sign-on, in its broad definition it typically includes issuing and revocation of common user identities and access rights automatically, and ensuring that all systems and applications in an organisation recognise these.
- IAM systems can link to Human Resources applications and organisation wide directories so that when personnel move jobs or change roles, the IAM system determines by means of automated rules how to adjust the individual's access rights in relevant applications and systems. Directory interoperability is therefore a key issue in IAM design.

- As IAM systems become more mature, it is clear they have a central role to play in securing collaboration and commerce. However, IAM systems work at the level of individual organisations; the requirement of interest here is linking IAM systems in different organisations together.

Issues

- IAM, as an automation technology, does not prevent the number of identifiers and associated access profiles continuing to proliferate as an organisation adds external user groups and applications. De-perimeterisation seeks to rationalise this situation.
- IAM interoperability can potentially be achieved at the level of directories, but the existence of multiple potentially conflicting directories is a real problem even within a single organisation. Data quality can in any case quickly degrade within a directory unless the supporting administration processes operate effectively. It does not help that the business case for building a directory or integrating multiple directories is often to reduce the administrative resources deployed within an organisation rather than increase them.
- Using directories for both internal and external identity management may cause many design and operational difficulties. Directory data can itself be sensitive. Directory technology sacrifices ease of schema modification for speed of retrieval, so redesigning a directory hierarchy to cater for re-organisation, or the addition of references to other organisations, is expensive. At a technical level, replicating data between directories, in the worst case multi-master replication, can impose unacceptable infrastructure overheads.
- IAM and/or directory interoperability also depends on common security profile definitions, or at least logical role and entitlement definitions. There is an infinite variety of these in practice. They have to be mapped to business roles and common access profiles. There may need to be extensive data cleansing to remove existing redundant access profiles held in existing applications and systems, and defined processes to ensure the organisation properly administers profiles in the future.
- Federated identity management schemes (Liberty Alliance etc.) focus on single sign on and access rights management at a technical level, but do not cover the wider aspects of IAM such as communicating responsibilities and liabilities between collaborating organisations to ensure they manage revocation, entitlements and accountability consistently. They also assume that users authenticate to one 'trusted' system and then 'pass through' to other connected systems, a model that may not apply well to collaboration and commerce universally.

Ease of resolution

- This is a long-term issue because IAM standards currently focus on internal IAM interfaces (e.g. for provisioning identities and security profiles into target applications and systems), not IAM system to IAM system interfaces. Jericho Forum will consider potential independent trust and identity models. One solution may be to unify IAM systems by importing common unique individual identities and potentially associated security profiles.
- Jericho Forum members can draw on considerable experience already of operating modern enterprise-wide applications such as ERP/CRM. In many cases these explicitly model people, organisations, organisation-wide processes, intra-organisational relationships and some entitlements (e.g. transaction authorisation responsibilities and financial limits and checks). The application technology has evolved to facilitate the job of implementing re-organisations and external access, but may well need to evolve further.

- Jericho Forum will also assess and work with the existing standards development groups for distributed IAM and directory interoperability as discussed above.

3.8.3 *Automate policy for controlled information sharing with other organisations*

Context

- Organisations define fundamental information security policies (to varying degrees of formality) in terms of the information classifications involved. A classification expresses the sensitivity and/or criticality of a particular type of information, and links to the organisation's view of the risks associated with compromising its security, and the control environment that the organisation expects will apply to that information.
- Classifications guide the evolution of organisational baselines for security controls and determine the norms for risk analysis and management. The fundamental reason to classify information is to ensure that there are organisation-wide rules for information security rather than leaving this up to the discretion of individuals.
- So long as information remains inside the organisation, personnel may only apply classifications loosely. However, as external access and disclosure requirements increase, classifications will provide an important method to define and enforce rules and constraints to control information sharing with business partners, suppliers and customers.

Issues

- Using formal classifications and data labels as a method to control data confidentiality (and latterly, integrity) has long been the subject of fundamental research and development in computer security. Mandatory access control schemes formed the basis of the US Trusted Computer Security Evaluation Criteria (the 'Orange Book') and derivative standards developed in the 1980s and 1990s. However, despite standardisation, these schemes have proven difficult to apply in practice and really only protect data within the confines of the 'trusted computing base' the Orange Book defines.
- There are four principal challenges in mandatory schemes:

  - determining their semantic intent and objectives: protecting users from potentially foolish actions, enabling the tracing and tracking of information (in which case applicability to the various representations of that information needs to be considered), or information flow control within the constraints of a given computing/communications system or systems

  - ensuring that they are logically sound and are sufficiently resistant to attack or bypass to make it worthwhile to automate them in the first place

  - capturing the complexities of actual organisational practice in an access control scheme, as opposed to formulating a scheme that is easy to automate (e.g. dealing with issues such as downgrades and aggregation of information from data in multiple files and records)

  - ensuring that a scheme can be applied with the minimum overhead on existing and off the shelf applications and systems.

- The overhead is that a label must be linked to the data it describes in a structured way, but this may mean labelling many files or records redundantly and ensuring that any software that needs to enforce the rules of the mandatory scheme uses the label to do this.
- Labels need maintenance and updating to support actions such as downgrading. As they encode classifications, the encoding method may need to be flexible in case the organisation decides to change its classifications or their meaning.
- While most applications deal with structured data, they do not support labels. Therefore, formally classifying and labelling data is not possible because there is no business demand to do it, and no demand can be created because of a lack of technical feasibility.

Ease of resolution

- This is an area for long-term standards development and influence over future vendor roadmaps. Research and development in this area has moved sporadically in recent years, and Jericho Forum will work within the specific context of collaboration and commerce in order to remain focused.
- The chosen starting point is the information architecture and data structuring standards developed by the World Wide Web Consortium (W3C) and others for the Semantic Web, which may offer the opportunity to capture and represent directly information flow control policies for collaboration and commerce.

3.8.4 *Harmonize identities and trust relationships with individuals*

Context

- Organisations and individuals face significant problems creating and managing logical identities and associated information. Often an organisation may 'know' the individual by several identities, and the individual will possess multiple identities issued by the organisations he or she deals with. These may be weak identities – such as the identity created when an individual signs onto a free Internet email service, or strong identities, such as a staff number in an organisation (but strength here is relative to that organisation).
- Identities therefore intimately relate to systems and security domains, such as the login identity that most computer users have to supply to sign onto an operating system or application. In turn, they are bound to the trust relationships the individual has with organisations, and other individuals. These drive the strength of the credentials involved, and the access that the individual is entitled to once authentication is successful.
- De-perimeterisation places considerable emphasis on the individual and strong identification of the individual. Efficiencies and cost savings cannot be realised unless the management burden of identities and trust relationships can reduce.

Issues

- The primary use of identities in systems is to facilitate authentication, and the proliferation of machine identities stems from the universal requirement to establish and maintain authentication credentials for users. It is difficult to decouple identities, credentials, trust relationships, authentication methods, and entitlements.

- Single sign on is driven by requirements to maximise user convenience. Its weakness is that the strength of identity, credentials, and trust relationship required is the highest common factor of any trust relationship needed for the lifetime of the session/transactions single sign on supports. On the other hand, transaction-level authentication is more invasive for the applications involved.
- Many people see directory interoperability as the foundation for harmonizing identities and trust relationships. Unfortunately, directories concentrate the issues rather than reducing them, as discussed above. Conventional ideas about role based access control assume that there is open knowledge within the organisation about who each role holder is. For secure collaboration between organisations, this may be sensitive information; or more simply, unacceptable overhead may be incurred to maintain role holder mappings across multiple organisations.
- Practical collaboration and commerce involves flexibility: as the parties gain more confidence in the business relationship, a higher level of trust evolves. There is also an overriding concern that the credentials and other security mechanisms involved must be cost effective and just sufficient for the current need at any given time.
- Efforts to promote collaboration and commerce between organisations must depend on enforceable responsibilities and liabilities. The other side of a trust relationship is the sanctions that apply once it is broken.
- There are numerous competing and non-interoperable proprietary solutions for 'universal' identities. National government efforts to develop electronic identity cards with strong identities fall into this category (viewing the nation-state as a 'proprietary' entity). In particular, unless a government has developed a commercial model for shared usage of strong identities with commerce, there is no local framework available to establish mutual responsibilities and liabilities underpinned by contract.
- There are legitimate privacy concerns about issuing 'universal' identities, as these allow tracking of an individual's on-line behaviour. If the strength of the identity depends on a single secure credential store, then breaching the store's security will breach the security of every system, application and organisation that uses the 'universal' identity. If a public digital certificate records the identity, presenting the certificate as part of authentication allows linking and tracking the sessions or transactions involved, even if the certificate contains no human readable information.

Ease of resolution

- This is a long-term issue, related to a number of the preceding business scenarios. Resolving it will realise the concept of 'individual-centric security' introduced in section 2. Jericho Forum will take a primary role in developing standards in this area. The initial focus will be to consider suitable trust models that balance rights, responsibilities and liabilities, and provide for an equitable allocation of costs and revenues to underpin infrastructure and services.
- There are three potential starting points:

- Identity based encryption (IBE) is an elegant concept allowing arbitrary data as a public key (e.g. email address) and the generation of potentially multiple private keys to underpin specific trust relationships. There are various IBE implementations covered by a number of patents. Its drawback (as a concept) is the potential computational complexity of the resulting security protocols hence communication overhead. It may also perpetuate the PKI notion of a 'trusted' third party, although it places different obligations on the TTP.

- The Digital Credentials approach developed by Stefan Brands (from original work by David Chaum on electronic cash) addresses issues of both privacy and security supporting single sign-on, fine-grained access control and liabilities associated with credentials, selective disclosure, anonymity and ownership tracing. This technology is covered by a number of patents issued from 1996-2001 and is being brought to market during 2005. It may not be suitable as the basis for open standards, but it does illustrate the limitations of conventional PKI in addressing the de-perimeterised scenarios Jericho Forum envisages.

- The Open E project has developed an important body of work on distributed identities, trust relationships and contracts, implemented by the E Language. This allows the development of minimally secure persistent distributed programs based on capabilities. Part of E is the concept of 'pet names': making the distinction between a strong identity needed for electronic authentication, a human readable identity that the individual can disclose, and the 'pet names' to use for particular trust relationships.

4 Jericho Forum's Roadmap

4.1 *Introduction*

Jericho Forum will achieve its mission through a number of Working Groups. These will develop the identified business scenarios further, and address the implied architectural considerations. They will also consider the ICT project lifecycle stages where standards, guidelines and the availability of working solutions that meet the standards will be most relevant.

4.2 *Working Groups, Outputs and Vendor Consultation*

There are six initial ***Working Groups***, each with its own charter. Further Working Groups may be added as required, or existing ones may be subdivided. Once it fulfils its original charter, a Working Group will either disband or extend its charter in order to contribute further towards Jericho Forum's overall mission.

Working Groups will produce various outputs, leading to principles and standards. Jericho Forum ***principles*** will be the highest level of expression of solutions to the issues it considers. Principles may:

- Define technical or other attributes of applications, systems or architectural components
- Be recipes for system, application or architecture development, and so relate to the process of implementation/evolution rather than a property of the implemented artefact
- Link to issues so that stakeholders can see the benefits of adopting each principle.

A principle may be strict (depended upon by other principles, or forming the rationale for a particular Jericho Forum standard), or simply an expression of good practice.

Jericho Forum ***standards*** will either endorse standards produced by other groups or define new ones. It will develop technical standards, which may include abstract models, protocol definitions, and application programming interfaces (APIs), if required, in collaboration with vendors, research groups and academia as appropriate.

Jericho Forum's ***Board of Management*** will oversee the Working Groups. It will control Working Group charters and work programmes, in consultation with the wider membership via general meetings, teleconferences and e-mail. It is responsible for setting up Working Groups, calling for volunteers to provide effort, and allocating research support and other resources to support their work. It will ensure that the technology and business issues tackled by Working Groups and their outputs address the business scenarios Jericho Forum identifies. It will own the present document, and update it from time to time as required. It will maintain up to date definitions of the business scenarios and Working Group charters, which will take precedence over the published version of this document.

Volunteers from the membership will lead and staff Working Groups. Any member can get involved, but only voting members (non-vendors) will be able to vote on and authorise Working Group deliverables.

Vendor consultation and involvement will use two mechanisms:

- Vendor members can get involved with Working Groups by contributing volunteer effort directly
- If vendor members are not currently directly involved (or a Working Group needs to consult more widely than the vendors who are involved), the Management Board will channel requests for information and input to the Jericho Forum Vendor Council.

The Working Group charters are introduced below. At initial formation, Working Groups will work on white papers such as the present document (which will exist in the public domain) and working documents (limited to Jericho Forum membership or within the Working Group itself). These white papers and working documents will identify further deliverables as appropriate.

4.3 *Meta-Architecture*

The Meta-Architecture Working Group will develop material to set out Jericho Forum's overall technical direction, focusing on principles and ensuring that these coherently define the de-perimeterisation approach.

Architectures will be 'consumers' of Jericho Forum principles and standards. In contemporary systems development, architecture concerns the process to translate business goals, objectives and requirements into technical definitions and requirements suitable for: constructing software; assembling hardware and software components into working applications and systems; and maintenance and adaptation of applications and systems as their requirements evolve.

This Working Group will be agnostic as to the architecture approaches that organisations may best use. An organisation seeking to adopt Jericho Forum principles and standards may focus on its enterprise ICT architecture, or just software architecture for a single system or application. This Working Group will focus on common concerns for any architecture:

- Viewpoints and views of individual stakeholders
- Architectural elements needed to construct applications/systems and their constituent parts
- Methods used to allocate security and functional requirements to these elements and resolve conflicting requirements (e.g. functionality versus performance)
- How Jericho Forum principles and standards can best facilitate architectural design.

It will consider enterprise or application/system project lifecycles to understand how Jericho Forum principles and standards map to relevant lifecycle stages, and it will define principles relating to each stage so that practitioners can understand how to apply de-perimeterisation...

It will define how de-perimeterisation affects applications/systems and their constituent parts (see sections 3.2 and 3.3) by mapping principles and standards Jericho Forum develops to each part.

It will focus on any business scenario Jericho Forum identifies that potentially has wide architectural impact or applicability, working in conjunction with other Working Groups to understand the implications.

4.4 *Requirements/Ontology*

Requirements/Ontology concerns capturing the broad spectrum of security and policy requirements for collaboration and commerce that Jericho Forum will address and their representation as abstract policy models. This Working Group will focus on business scenarios and policy management relating to controlled information sharing.

In particular, it will focus on security policies for information flows associated with collaboration and commerce within and between organisations, as these may be supported in the Semantic Web. The focus will be on confidentiality and integrity policies and controls, but with the recognition that accountability for access and other security objectives may also be relevant.

The Semantic Web, as a linked information structure potentially spanning multiple organisations and multiple information sources, clearly poses potential privacy and security concerns, so this Working Group will also focus on these.

This Working Group will consider the expression of requirements concepts including:

- Trust, threat and risk models that represent and generalise the issues from the business scenarios
- Data/information classification rules for corporate data:
- Collaboration and commerce processes (particularly web based) and their integrity and reliability requirements

It may also develop requirements for submission to W3C or other relevant bodies based on practical use of the Semantic Web and Web Services to support secure collaboration and commerce.

4.5 *Technology and Solutions*

In order for organisations to adopt Jericho Forum principles and standards, they must be grounded in practical solutions. This means that Jericho Forum must keep abreast of relevant issues that its members are encountering today when they engage in collaboration and commerce, and attempt to deploy ICT securely to support this. Members may be solving current problems with tactical solutions or perhaps trying to work around the problems in the absence of a solution. Above all, whatever standards Jericho Forum develops must be grounded in practical implementations and demonstrable solutions.

This Working Group will work closely with other Working Groups to ensure that technology assumptions are reasonable. It will focus on business scenarios relating to security interoperability.

In addition, engagement with current technology issues will be a springboard for vendor consultation. This will provide opportunities for both customer members and vendor members:

- Customer members can identify common issues and requirements and consolidate them
- Vendor members can explain how common issues and requirements can be tackled – or initiate developing solutions (whether short-term, tactical solutions; or long-term, strategic solutions) to meet a clear market demand.

The scope of the technology issues it will examine will include:

- Identity management technologies
- Private networking and remote access technologies
- 'Trusted platform' (digital rights management) technologies
- Protocols and formats
- Cryptographic support and key management systems
- Application programming and device interfaces.

Jericho Forum assumes that organisations will adopt the most commercially appropriate solutions to their needs, so will not endorse specific technology or products. However, this Working Group will involve determining the practicality and feasibility of standards by means of proof of concept and pilot projects, which will involve working with developers (whether they work for vendors or end user organisations) to build and test these.

Vendor members will be encouraged to demonstrate and validate solution interoperability, so that customer members can ensure that with very short lead times, devices and applications can be connected together securely and safely.

This Working Group will oversee proof of concept / pilot projects and interoperability testing ('bake-offs') in order to ensure the validation of standards and implementations is robust and realistic. It will also develop guidance, methods and worked examples to facilitate solution validation and take-up at minimum cost and business risk.

4.6 *Trust Models*

Key to the business scenarios is the fundamental requirement to establish trust between the parties involved in collaboration and commerce, both at the level of individuals (people and organisations) and systems/infrastructure. For any business relationship, the parties involved will need to assess security risks to select or confirm the security controls, sufficient for the level of trust they seek. . Frequently this is a slow process and a potential barrier to achieving any workable collaboration or commerce, as each party determines the desired level of trust, with no common frame of reference.

The aim of this Working Group is to define that common frame of reference and consider a variety of trust models that may be required for collaboration and commerce. It will develop a standard template, abstract model and supporting, iterative process that organisations can use to evaluate concerns and facilitate dialogue with collaborating and trading partners when designing services and formulating service agreements and contracts. It will focus on business scenarios relating to authentication and access.

Jericho Forum recognises that standards exist to support identity management, single sign-on and federated authentication. This Working Group will examine whether a single credential to identify, authorize and authenticate access and information flows can succeed in resolving the variety of interdependent business and technical requirements encountered in practice, to establish trust in:

- The individual
- The organisation to which he or she is affiliated

- Other organisations with which he or she has dealings, and issues relating to 'transitive trust'
- The location where he or she currently resides
- The computing device he or she is using
- The collaboration or commerce event-specific context of the moment.

It will consider the need to support the security control decisions associated with system or network access, the right to invoke a function or transaction, facts and attributes about a party involved that are independent of their name/identity (such as age, sex, voting preference etc), time dependent qualities or capabilities, or a combination of these.

A critical factor that will determine take-up of trust models is the extent to which they adjust to reality when trust breaks down. The Working Group will therefore take into account notions of dynamic trust, and the potential to determine what level of trust is appropriate dynamically.

4.7 *Management and Monitoring*

Founder Jericho Forum members have succeeded in realising significant business benefits from moving to an open network model. Cost effective systems management remains a challenge because some routine system housekeeping has become the responsibility of end-users. Some management capabilities can function semi-automatically in this environment, e.g. anti-virus updates. However, unless all system management and monitoring tools can function securely over open networks, organisations' ability to exploit them will be impaired.

In a de-perimeterised scenario, organisations and individuals engaging in collaboration and commerce will suffer security incidents of various kinds. There is a need to evolve existing approaches, techniques, tools and technology to enable incident handling spanning multiple organisations and individuals.

This Working Group will initially focus on business scenarios relating to:

- Remote management and monitoring
- Remote device and user management
- Malicious software incident detection, containment and remediation between organisations
- Patch management
- Security status monitoring and incident handling.

Organisations adopting an open network model need to be able to manage and support IT platforms securely. This will be especially true for internal collaboration, but may also apply to external collaboration and commerce if this requires deployment of software or hardware platforms from one organisation to others.

This Working Group will aim to evolve existing management and monitoring technology deployed in closed networks to allow secure management and monitoring in an open network environment.

4.8 *Public relations (PR) Media and Lobbying*

Jericho Forum's PR media and lobbying Working Group exists to ensure that Jericho Forum gets its message presented effectively. Its goals are:

- Attract additional members
- Publicise Jericho Forum's mission, scope and activities
- Keep abreast of relevant regulatory developments
- Engage the attention of vendors (whether as prospective members or in the promotion of Jericho Forum principles and standards)
- Provide timely comment on relevant issues

In addition, as Governments are potentially significant stakeholders who may benefit from Jericho Forum's activities, the PR media and lobbying working group will lobby relevant Government ministries, departments and agencies (e.g. standards agencies) to achieve closer collaboration and consultation between them and Jericho Forum.

Part of Jericho Forum's mission is to support, and act as an advocate for, the responsible, private and secure exploitation of ICT for consumer and other private data. The PR media and lobbying working group will provide the focus for this activity.

4.9 *Relationship of business scenarios to Working Groups*

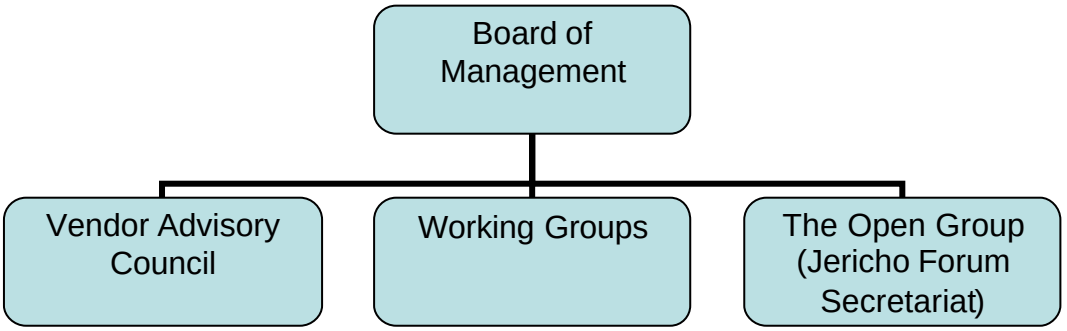
The business scenarios set out in section 3 relate to the Working Groups as follows. A 'tick' indicates that the scenario is of concern to the Working Group.

Scenario	**Meta Architecture**	**Requirements/ Ontology**	**Technology and Solutions**	**Trust Models**	**Management and Monitoring**
Access over wireless and public networks			v		
Domain interworking via open networks			v		v
Phoning home from a hostile environment			v		
Enable portability of identities and data	v	v	v	v	
Application access by suppliers etc.			v		
Outsourced help desk access			v		v
Connect organisations using XML messaging	v		v	v	
Consolidate IAM systems	v		v	v	v
Automate policy for controlled information sharing	v	v		v	
Harmonise identities and trust relationships	v	v		v	

5 Taking the vision and mission forward

5.1 *Jericho Forum Structure*

Jericho Forum is organised as follows:



5.2 *Jericho Forum Processes*

The Board of Management will meet approximately six times per year to review the overall operations of Jericho Forum, financial status and plans, and outlook. Further details of the responsibilities of the Board of Management are set out in the Memorandum of Agreement (MoA) document.

Working Group and Vendor Advisory Council activities are discussed in section 4 above.

Jericho Forum will convene general meetings/workshops 2-3 times per year to progress and discuss the work programmes of the working groups and other matters of interest to the membership. At least one of the 2-3 meetings will be held in the US, the remainder in Europe or Asia-Pacific, depending on member demand.

Jericho Forum will review this visioning white paper every 12-18 months to assess progress. In addition, the Board of Management will monitor the individual progress of each Working Group, forming, merging and disbanding Working Groups as it judges necessary to achieve the mission.

Jericho Forum will charge subscriptions for membership to fund administration, IT support, promotion, publicity and programme management for the Working Groups. Jericho Forum will seek sponsorship and grants to fund proof of concept and pilot projects, which will be financed on a cost-neutral basis. It will also disburse funds to support applied research, and for other purposed pursuant to its vision and mission, as the Board of Management sees fit. It will publish an annual report to the membership setting out its financial affairs and summarising the activities of each year.

5.3 *Joining Jericho Forum*

Jericho Forum actively seeks new members to participate in its activities and meetings. Membership grants access to all working group activities and documents. Membership information can be found on the Jericho Forum website, www.jerichoforum.org

6 Glossary and Acronyms

Glossary

authentication	the verification of a claimed identity for an individual person, system, process, or originator of a communication.
authorisation	the granting of rights for an individual person, system, or process to access information or initiate a function or action.
Basel II Accord	risk management standard for financial institutions published by the Bank for International Settlements in Basel, Switzerland. It covers market, credit, and operational risk, and further defines the latter to include any risk of loss from inadequate or failed internal processes, people, systems, or from external events".
certification	a) the process of substantiating claimed qualities and properties associated with a cryptographic key; b) the authorisation of the results of an evaluation (q.v.) by a competent authority (e.g. to confirm the evaluation was undertaken by a party independent of a product's or system's developers or sponsors).
cookie	a data element included within HTTP messages and capable of being stored by a browser to record web surfing activity, transaction data or other information concerning web site or web page access.
classification (data/information)	the indication of the need, priorities, and degree of protection required for data/information
cryptography	mathematical techniques, including encryption and digital signatures, which can be used to achieve various aspects of information security.
de-perimeterisation	the act of applying organisational and technical design changes to enable collaboration and commerce beyond the constraints of existing perimeters, through cross-organisational processes, services, security standards and assurance
digital signature	a data item, associated with other data (e.g. a message or file) that allows that data's integrity to be determined and allows the data's owner, originator or creator to be authenticated; typically using public key cryptography and therefore also supporting non-repudiation for the owner, originator or creator.
encryption	transformation of data in order to render it unintelligible except to authorised recipients or accessors (i.e. those possessing a copy of the appropriate encryption key)
evaluation	independent review, assessment, verification, validation and/or testing of a product or system for the purpose of reporting on security capabilities and the likelihood of their correct functioning
firewall	system designed to prevent unauthorised access to or from a private network
Gramm-Leach-Biley Act	US privacy legislation regulating financial institutions
grid computing	technology and standards for co-operative parallel computation conducted by multiple applications and systems
HIPAA	Health Insurance Portability and Accountability Act – US privacy legislation regulating healthcare providers and institutions, and health insurance providers
home office	A place of work that is also a place of residence for an individual.
information security	preservation of confidentiality, integrity and availability of information NOTE Confidentiality is defined as ensuring that information is accessible only to those authorised to have access. Integrity is defined as safeguarding the accuracy and completeness of information and processing methods. Availability is defined as ensuring that authorised users have access to information and associated assets when required.

'man in the middle'	a malicious attack on a communication system whereby the attacker is interposed between the legitimately communicating parties with a view to capturing and perhaps modifying the message traffic between them; or using the information gained (e.g. passwords or cryptographic challenges) to support further attacks
non-repudiation	the inability of a communicating party or originator/creator of data to deny that the communication or data creation was, in fact, initiated, participated in or caused by them; typically achieved by means of digital signatures relating to communicated messages or data
open network	a network freely accessible at low or no cost to arbitrary communicating parties, such as but not limited to the public global Internet, with few or no inbuilt information security controls protecting the use of that network (although the network infrastructure itself will typically have some protection in order to support the provision of a service of useful quality)
password synchronisation	automatic updating of passwords for multiple systems / applications so that each user only needs to remember a single password to access any system/application
public key cryptography	cryptographic technique based on the use of pairs of public and private keys, whereby data encrypted using a public key can be decrypted only by the corresponding private key (and depending on the technique used, vice versa); also known as asymmetric cryptography
policy management	automated creation, maintenance and enforcement of rules for information security such as rules for access to systems or data; typically implemented to facilitate the administration of multiple networks, systems or applications from a single point
privacy	rights of individuals to be free from unreasonable interference or intrusion, and in particular to determine or be consulted on what of their personal information can be communicated, and to whom
proxy	a process or application that acts as a relay between source and destination systems, processes or applications, typically within a network communication path and typically capable of achieving various aspects of information security for that communication path
re-perimeterisation	continuing to apply de-perimeterisation (q.v.) to ensure that security processes and controls maintain and uphold confidence in cross-organisational collaboration and commerce, however the organisation(s) involved grow and change
single sign-on	a system permitting users to log on and interact with multiple applications or systems while only needing to authenticate once.
'spoofing'	a form of malicious attack on a communications system in which an attacker assumes the logical identity of a legitimate communicating party with a view to deceiving other communicating parties that the attacker is the legitimate owner of that identity; also referred to as 'masquerading'
'transitive trust'	The concept illustrated by the question: If A trusts B, and B trusts C, can A trust C?'

Acronyms

API	Application Programming Interface
B2B	Business-to-Business
B2C	Business-to-Customer
B2E	Business-to-Employee
B2P	Business-to-Public
B2G	Business-to-Government
COTS	Commercial Off-The-Shelf
CRM	Customer Relationship Management

DR	Disaster Recovery
EDI	Electronic Data Processing
ERP	Enterprise Resource Planning
G2P	Government to Public
GLBA	Gramm-Leach-Biley Act
HIPAA	Health Insurance Portability and Accountability Act
HL7	Health Level 7
HTTP	Hyper-Text Transfer Protocol
IAM	Identity and Access Management
IBE	Identity Based Encryption
ICT	Information and Communications Technology
IETF	Internet Engineering Task Force
IP	Internet protocol
IPSec	IP Security
LAN	Local Area Network
MPLS	Multi-protocol label switching
MoA	Memorandum of Agreement
MoU	Memorandum of Understanding
MPLS	Multi-Protocol Label Switching
NAT	Network address translation
P2P	Peer to Peer
PDA	Phone/Personal Digital Assistant
PKI	Public Key Infrastructure
PKIX	IETF acronym for Internet PKI standards based on X.509
PR	Public Relations
SAML	Security Assertions Markup Language
SOAP	Simple Object Access Protocol
SSH	Secure SHell
SSL	Secure Sockets Layer
TCP	Transport Control Protocol
TTP	Trusted Third Party
VPN	Virtual Private Network
WAN	Wide Area Network
WS-Security	Web Services Security - Series of W3C standards for communications security for web services based on SOAP
W3C	World Wide Web Consortium
XML	Extensible Markup Language