CABINET OFFICE

Office of the *e-Envoy*

Leading the drive to get the UK online

delivering UK online

HMG Public Key Infrastructure - Overview

Version 1.0
December 2002

Executive Summary

A high proportion of business within government is carried out electronically, exploiting, amongst other things, email and attachments. There is a strong requirement to keep some of this business private and to ensure that documents are coming from the originator without being altered and without their origin being denied at some future date.

We are encouraging citizens and businesses to use electronic government services but at the same time we acknowledge that they are distrustful of interacting in this way. It is therefore essential that government can simply authenticate itself to the people and businesses that transact with it to build trust and confidence.

The Office of the e-Envoy is co-ordinating the establishment of a pan-government Public Key Infrastructure (PKI) that will be a strong enabler for building this trust and confidence within the government domain and providing a convenient mechanism for government to authenticate itself to those outside.

Some government departments have independently identified the need for the features a PKI can deliver and the Office of the e-Envoy would strongly recommend they become part of the HMG PKI to realise the following additional benefits:-

- Government bodies often need to work together and this will be seamless if there is a co-ordinated approach to implementing PKI.

- Achieving a high degree of interoperability within government at the outset would realise significant savings over seeking to achieve it retrospectively.

- The ‘HMG Brand’ is well known and a single government trust point will make the process of government authenticating itself to citizens and businesses simpler.

- There are large potential cost savings to be made by exploiting larger scale purchases and benefiting from the propagation of best practice.

It is essential that those in the departments responsible for establishing their own PKIs read this document and know they can join a wider pan-government community with additional benefits. In addition it is important that there is a wider awareness that there is an HMG PKI so that departments know where to go if they need to exploit a wide body of expertise.

Contents

1. Introduction

The government has set a target of providing all its services electronically by 2005. It is of paramount importance that this is done securely to ensure the protection of sensitive public data, and the establishment of a common trust hierarchy for government is a step towards achieving the required level of security.

The first section of this document describes in general the features, benefits and implications of a PKI. Section 2 goes on to explain what the HMG PKI is, and the advantages of belonging to it if you are considering providing electronic services for or on behalf of government. A comprehensive list of abbreviations is attached at Appendix A to aid in the understanding of this document.

2. Public Key Infrastructure (PKI)

2.1. What does PKI do?

It provides users and applications with underlying "Trust".

2.1.1. A Public Key Infrastructure (PKI) provides users and applications with an underlying "trust" that is essential for providing secure e-business and e-government services. PKI offers the following security services:

a) authentication;

b) integrity;

c) confidentiality; and

d) non-repudiation.

2.1.2. **Authentication** is the process of proving or verifying certain information. Commonly this is used in the confirmation of an individual's identity to ensure they are who they say they are. Authentication is also used to validate other attributes of an individual rather than their identity – such as their age group, membership of certain groups, security clearance status, etc. The object of authentication does not have to be an individual – details of a document's origin or the destination of an article in transit, are other attributes that may need to be validated.

2.1.3. **Integrity** in this context refers to the process of ensuring that information cannot be deleted or modified in any way. It is important to know that a message that has been received is identical to the one that was originally sent. A PKI makes it possible for documents to be published such that their integrity can be verified by a potentially unlimited number of recipients.

2.1.4. **Confidentiality** (or privacy) is the process of preventing unauthorised users from reading information. Confidentiality is achieved by encrypting the original information making it unintelligible to anyone, other than authorised receivers, who can decrypt to restore the original information.

2.1.5. **Non-repudiation** is the process of proving, beyond denial, to a neutral third party that an event occurred. For example, this may be useful following placement of an order, to ensure that it cannot be denied once delivery has taken place.

2.1.6. **Authorisation** is a related service and is the process of determining what you are allowed to do. While PKI does not provide directly for authorisation, it is obviously essential to have a strong authentication process before authorisation can be given to perform actions with a high impact.

2.2. What are the important features of PKI?

Cryptography to stop the data being read by unwanted people, digital signatures for confidence in the data originator and in the content integrity, and certificates to determine the level of trust.

2.2.1. PKI is built around, and includes the use of, **public key cryptography** – a form of cryptography in which there are two keys: one that is publicly available (known as the **public key**), and a second that is kept secret at all times (known as the **private key**). The two keys are mathematically linked, but in such a way that it is not possible[1] to calculate the private key from the public key.

2.2.2. One of the most beneficial features of PKI is the **digital signature**, which is made possible by having the two keys. The private key is used to create an unforgeable fingerprint of the data to be signed, so providing a means of determining both authenticity and integrity. If used in the correct manner digital signatures can also provide for non-repudiation. There are a number of benefits of digital signatures over real-world signatures.

a) Digital signatures are firmly bound to the data they relate to. It is not possible to remove a digital signature and apply it to a different document.

b) If there is any change at all to the content of the document after the digital signature has been calculated (even changing one letter), the digital signature will be invalidated.

c) Anybody can validate the digital signature because this is done using the public key. However, this does not enable them to forge the digital signature because this can only be done with the private key.

2.2.3. Confidentiality is also provided through the **encryption techniques** employed by PKI. The public key of the recipient is used to encrypt the data to be sent. The encrypted data can only be decrypted using the corresponding private key, ensuring that only the authorised recipient can access the original message.

2.2.4. A **certificate** is used to link the name of an individual or other entity (known as the certificate subject) to its public key. The subject of the certificate is also known as the certificate holder, certificate owner, **end entity** or **subscriber**. The certificate is used by the subscriber to perform a secure transaction with another end entity – known as the **relying party**.

2.2.5. While public key cryptography is practically impossible to break using brute force techniques, there are many other aspects that need to be in place to provide the security and trust required to support business processes. In particular:

a) subscribers must keep their private key safe and ensure that there is no unauthorised access to it;

---

[1] Strictly speaking this should read 'computationally infeasible'. However, this can be interpreted as impossible for practical purposes – if all the computers in the world attempted to crack a 2048-bit RSA key pair, they would still require far longer than the age of the universe to perform the task.

b) relying parties must be confident that the subscriber's private key is safe;

c) relying parties must use the public key that corresponds to the entity that they want to transact with; and

d) relying parties must be confident that they are using the appropriate public key.

2.2.6. A trusted third party is an essential component of PKI, and acts to provide the levels of trust described above. This trusted third party is known as a **Certification Authority** (CA) and issues certificates to end entities, digitally signing them to ensure their integrity. The CA uses the services of a **Registration Authority** (RA) to verify the identity of the individual before the certificate is issued.

2.2.7. The rules that describe the applicability of a certificate, and the security procedures and techniques used in its management, are contained in a **certificate policy (CP)**. Each certificate is issued under at least one certificate policy which forms the basis for interoperability within the PKI. A relying party will refer to the certificate policy to decide whether the certificate can be trusted as the basis for the desired transaction.

2.2.8. Certification Authorities (CAs) can be chained together to form a certification path or 'chain of trust'. Typically this takes the form of a hierarchy where the CA at the top (or root) of the hierarchy acts as the overall trust provider (known as the **trust point**), and certifies the trustworthiness of subordinate CAs. A relying party will have one or more trust points that they explicitly trust – when they wish to validate an end-entity certificate they trace the certification path back to a valid trust point. Note that while this trust point is typically the top of the hierarchy, it does not necessarily need to be at the top and can equally be a subordinate CA.

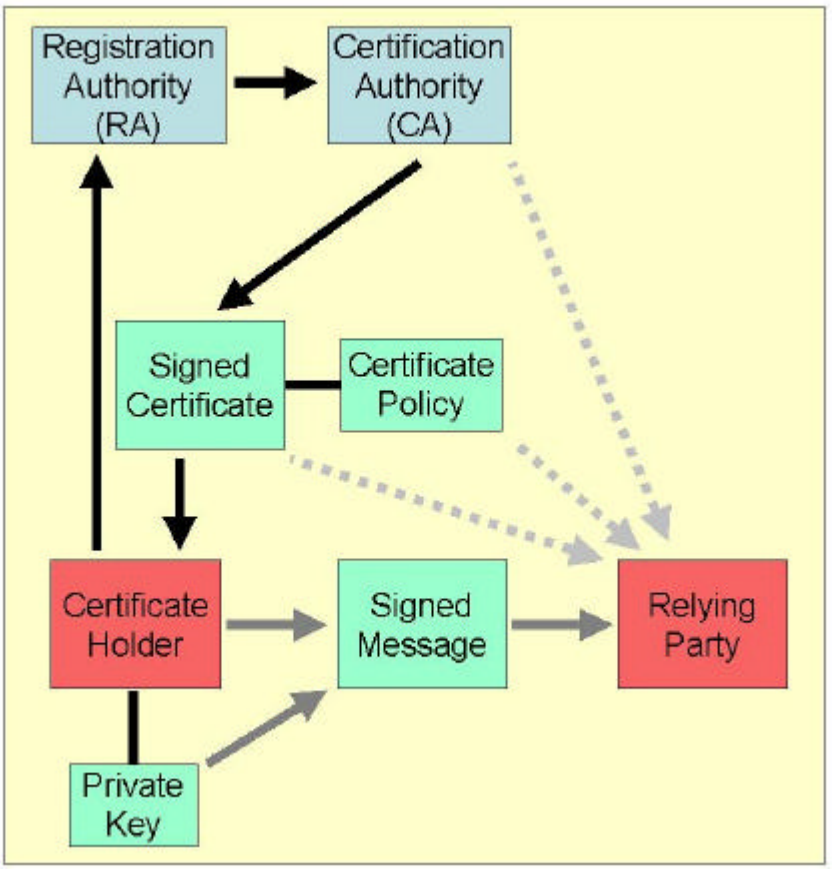

Figure 1: PKI for digital signatures

2.2.9. *Figure 1* shows how PKI works for digital signatures.

a) The black arrows show how an individual applies for a certificate through a Registration Authority and is issued with a certificate signed by the Certification Authority.

b) The dark grey arrows show how the private key is used to sign and send a message.

c) The dotted light grey arrows show the information used by the relying party to assess the validity of the signature and decide whether to trust the message.

2.3. What are the advantages of PKI?

It is an established technology that is more secure and easier to use than alternative techniques.

2.3.1. The Government is committed to making all its services available electronically by 2005. Substantial cost and time savings can be made through the use of e-business processes, both within the public sector and externally with the private sector and other governments.

2.3.2. It is essential that these services and processes are achieved without compromising the confidentiality and integrity of the information concerned, and that their availability cannot be compromised through malicious activities. It has been determined that 20% of these services will require strong authentication. If sufficient security is not applied at an early stage in the development of these services and processes, there is a high risk of financial liability damages, legal disputes or adverse publicity.

2.3.3. The security functions described in Section 2.1 are vital components of the overall security of these e-business systems.

2.3.4. There are three concepts which can be used as the underlying basis of the authentication technology for identifying an individual:

a) **knowledge:** something you know, such as a password or PIN;

b) **possession:** something you have, such as a PKI private key; and

c) **characteristic:** something you are, such as a fingerprint or retina scan biometric.

2.3.5. Passwords and PINs are the traditional solution for authentication. However, it is not possible to provide a high security authentication system using passwords or PINs alone. Problems with passwords include:

a) many passwords are badly chosen and can be broken within minutes using easily available technology;

b) even well chosen passwords are generally not sufficiently long to prevent compromise by a committed attacker;

c) long passwords are not easily remembered and have ease-of-use problems – they tend to be written down, compromising security greatly;

d) because passwords need to be easily recalled, they are extremely susceptible to social engineering attacks such as shoulder surfing or masquerading;

e) because passwords need to be shared between the parties concerned, separate secure interactions with multiple parties requires the use of multiple passwords – this can result in a management overhead and a security risk;

f) passwords must be communicated between the interacting parties, resulting in an increased risk of password interception or unauthorised access to password databases on authentication servers; and

g) many implementations of password systems are insecure.

2.3.6. Biometric technology is relatively new and is often used for ease-of-use rather than for security. Problems with biometrics include:

a) systems are susceptible to spoofing whereby an attacker fools the system using some sort of prosthetic device – the extent to which this can be used is dependent on the actual biometric used;

b) systems are susceptible to replay attacks whereby an attacker captures a legitimate data stream and replays it to the host computer, bypassing the biometric device;

c) biometrics are not suitable for certain environments (e.g. fingerprint recognition systems are not suitable when the users are required to wear gloves);

d) because biometrics are fundamental to an individual, there are problems with revocation;

e) biometric technology is relatively new and so there is insufficient assurance that all the vulnerabilities have been identified and analysed; and

f) there is a lack of deployed systems and infrastructure for biometrics.

2.3.7. The Security Framework documents[2] describe four levels for registration, authentication, confidentiality and trust services (covering integrity and non-repudiation). All e-government services should be assessed with respect to this framework: Level 0 services are essentially anonymous and Level 1 services are sufficiently low impact that weak authentication methods such as passwords can be used. However, services that are categorised at Level 2 or 3 should use the strong authentication and trust services provided by PKI.

2.3.8. PKI technology is a relatively mature technology that represents the most secure method of authentication. Additionally, security can be increased through the use of a cryptographic smart card to store and process the private key, and by combining the PKI with password and/or biometric methods (known as 2 or 3-factor authentication).

2.3.9. PKI is particularly useful for protecting the integrity of information. The private key is only required at publication time and so the integrity of the information can be verified using only the public key – this can be done by a potentially unlimited readership base.

2.3.10. PKI is more flexible than traditional methods for maintaining the confidentiality of information. In the traditional approach to confidentiality, pair-wise key-exchange is required between every combination of communicating parties that need an exclusive private conversation, prior to the establishment of a secure communication. PKI does not require this and is much more suitable for the creation and management of dynamic and flexible trust relationships.

2.3.11. With an appropriate implementation, using methods such as secure time-stamping and assured client technology, PKI can be used to support strong non-repudiation, suitable for use in legal situations and in place of traditional physical

[2] Documents can be found at http://www.e-envoy.gov.uk/oee/oee.nsf/sections/frameworks-top/$file/frameworksindex.htm

signatures. Non-repudiation is an essential component for many high-impact services and processes. There are no other technical solutions that can provide similarly strong levels of non-repudiation.

2.4. What are the risks of ignoring PKI?

The security of e-government transactions may be compromised and alternative approaches to implementing effective security may lead to inferior systems, which will not achieve the modernising government objectives.

2.4.1. If PKI is not adopted, the major risk is that the e-business and e-government systems set up will be insecure. Although PKI does not address all aspects of e-security (such as technology to prevent attackers exploiting software vulnerabilities to hack into systems), it is a vital component in a well-engineered secure e-business or e-government system. Future compromises in security can result in major financial and legal implications, as well as adverse public relations.

2.4.2. PKI security is an enabler for maximising access to information and services. Without PKI, there is a high risk that other security measures will result in inflexible systems with low functionality. Opportunities to exploit e-business and e-government technologies to reduce costs and improve performance may be lost.

2.5. What are the main issues associated with implementing PKI?

Investment in overcoming problems associated with its large scale implementation and in developing coherent policies and procedures. Costs will be incurred in registering and managing users. The HMG PKI is helping to address these issues.

2.5.1. PKI has the potential to provide strong security services as described previously. However, the implementation of PKI is not trivial and there are a number of issues associated with the successful roll-out of PKI. The main issues are as follows:

a) While closed implementations of PKI are relatively mature, PKI technology and processes for open systems[3] are still maturing. There are very few proven solutions on a large scale and many implementations do not use the full features specified in the PKI standards.

b) The interoperability of PKI products is not universal. Some PKI standards have ambiguities which have been interpreted in a number of ways by different PKI product vendors.

c) There is a cost associated with the implementation of PKI, particularly with the registration and management of end entities. This cost can be significant, although it is generally substantially smaller than the total cost of ownership of the IT solution.

d) Policies and procedures need developing. If these policies are not developed in a coherent manner, there is the potential for non-interoperability due to policy and configuration issues, even if the core PKI technology does interoperate.

e) There are a number of cultural changes that are required in any organisation that takes up PKI technology. New methods of working require user training and user acceptance, and best practice in these areas has yet to be identified.

2.5.2. Section 3 describes how the HMG PKI is addressing the issues mentioned above. In particular policies are being developed and best practice is being identified. Additionally the economies of scale associated with a consistent HMG wide approach will help address the issues of interoperability and of large open PKI systems.

---

[3] An open system is one in which certificate holders can use their certificate to facilitate transactions with numerous and potentially unlimited other parties. A closed system is one in which the certificates are used within a bounded context. In a closed system, a contract or a series of contracts identify and define the rights and responsibilities of all parties to a particular transaction.

3. HMG PKI

3.1. Why do we need an HMG PKI?

The two competing options for providing a pan-governmental PKI are either to implement it under full government control or to rely on a third party trust provider. The former option allows us to determine who is included and under what conditions and will make it easier to authenticate HMG to other governments and also to businesses and individuals.

3.1.1. Section 2.3 outlined the reasons why PKI is an essential component of e-business and egovernment. In the fullness of time, PKI will need to be available across government to support internal communications, internal business processes, communications and commerce with the private sector, services to citizens, communications with other governments, etc.

3.1.2. This pan-governmental PKI capability can, however, be achieved in a number of different ways. Rather than implementing an HMG PKI, an alternative option would be to issue government employees with certificates from a commercial PKI (e.g. Verisign, or from a tScheme[4]-approved trust provider such as the BT Ignite On-site service).

3.1.3. The advantage of an HMG PKI is that HMG has control over who is included in the trust domain (i.e. who is trusted) and the certificate policies used (i.e. to what extent they are trusted and the relevant conditions, obligations and liabilities). This is particularly important as these policies underpin the legal framework within which the certificates are used. The use of third party certificates would mean that the third party trust providers would have this control, potentially leading to undesirable trust relationships and liabilities.

3.1.4. It is important that relying parties have trust in the HMG certificates. If third party certificates are used, then the relying parties must also be able to trust this third party in addition to trusting HMG itself. This may cause problems with trust relationships, particularly with respect to relationships with other governments.

3.1.5. It is more effective to carry out the registration of certificate holders in-house, as HMG is best placed to verify the identity of its own staff. It is also advantageous to maintain control over the registration information that appears on the certificate, such as the departmental position of the certificate holder. This degree of control is facilitated by the operation of the HMG PKI.

3.2. What does it mean to be a member of the HMG PKI?

The HMG PKI will be a symbol of pan-government co-operation and corporacy with respect to secure electronic transactions. Being a member will place an organisation within a large trust community that includes central government departments, local authorities, NDPBs and potentially private sector organisations and will allow them to transact seamlessly with one another.

---

[4] tScheme is a voluntary, industry-led, co-regulatory scheme established to provide accreditation services delivered by Trusted Service Providers. More details can be found at http://www.tscheme.org/

3.2.1. A certificate authority that is part of the HMG public key infrastructure is a member of the HMG trust domain. The consequence of this is that a relying party that receives an HMG PKI certificate will trust that the certificate is valid for the identified individual (according to the level of assurance specified in the certificate policy), provided that they trust HMG and the HMG PKI.

3.2.2. The ownership of an HMG PKI certificate does not necessarily imply that the owner is a member of HMG, although this information can be included in the certificate if required. Similarly, the ownership of an HMG PKI certificate does not imply that the owner is authorised to conduct business on behalf of HMG. In certain circumstances it may be suitable to include this authorisation information directly on the certificate; alternatively authorisation information may be provided using separate techniques or systems.

3.2.3. The implication of this is that the scope of the HMG PKI will be large, covering central and local government, other public sector and non-departmental public bodies as well as, potentially, the private sector. The certificates will only be used to facilitate transactions for or with HMG and so many of the benefits of closed PKI systems will apply to the HMG PKI.

3.3. What are the advantages of membership of the HMG PKI?

Cost savings could be realised by the re-use of certificate policies, the potential to exploit pan-departmental application purchases and the sharing of best practice between departments. Problems of interoperability between organisations should also be reduced.

3.3.1. Membership of the HMG PKI will provide cost and resource savings through the use of standard HMG-wide certificate policies, reducing the need for departments to create the certificate policies themselves and greatly simplifying the process of implementing PKI.

3.3.2. These standard certificate policies will also help to ensure interoperability when communicating across government, enabling application solutions such as pan-governmental secure e-mail.

3.3.3. Interoperability with external organisations will benefit as it will be easier and more cost effective in many cases to form external trust relationships at the HMG-level rather than multiple relationships at department level.

3.3.4. Maximising the use of certificates and policies in this way has corresponding benefits for the users, as the number of certificates that they will be required to hold will be minimised. This helps with ease-of-use and reduces the burden of managing the certificates once they have been issued.

3.3.5. There is the potential for services to be provided centrally for issuing and managing certificates. This could reduce costs dramatically for those departments that have standard requirements and are able to use the HMG-wide certificate policies.

3.3.6. Membership of the HMG PKI enables departments to exchange expertise and best practice on PKI issues through workshops, discussion forums and other collaborative techniques. This will reduce the time and resources required to implement PKI, and help to reduce the risk of inappropriate solutions.

3.4. Is the HMG PKI secure?

The HMG Root Certification Authority is off-line and is based at CESG, the UK government's national technical authority for information assurance.

3.4.1. The HMG Root Certification Authority has been built and operated with a high degree of security. It is operated by CESG who have established high security practices covering physical, personnel, procedural and technical security measures. In particular, the CA is off-line and cannot be attacked by electronic

means, and is housed within a secure underground area with substantial surrounding physical security. Cryptographic key material is generated by CESG using assured hardware modules and imported into the Certification Authority software, to ensure high security.

3.5. Will certification by the HMG PKI require substantial cost, time and resources?

Some costs will be incurred but the benefits of being part of a larger group should produce cost savings compared to the alternative of each department working on its own.

3.5.1. Although there will be some time and resources associated with the certification process, these are offset by the savings that can be made through exploiting best practice and re-using policies and procedures that have been developed throughout HMG. In particular the fact that HMG-wide certificate policies will be available, along with the key trust relationships that accompany them, will lead to substantial savings.

3.6. Will membership of the HMG PKI restrict us in our activities?

No. It is intended to maximise its applicability and also to allow departments the flexibility to independently exploit PKI for their own business needs.

3.6.1. The HMG PKI provides an overall framework within which a cohesive and consistent approach can be ensured. The scope of the PKI has been defined to be as large as possible to maximise its applicability, and so in many cases the HMG-wide certificate policies will be suitable for all a department's needs.

3.6.2. However, the approach includes a high degree of flexibility and allows individual departments to define their own certificate policies for internal use. It is not intended that membership of the HMG PKI will prevent a department from using PKI to support its own particular applications and requirements.

3.7. How will the HMG PKI be set up?

The HMG Root CA, run by CESG, will be at the top of the hierarchy beneath which will be the departmental CAs. Overall control will be vested in the Policy Management Authority (PMA) which will be populated to represent the interests of the different organisations within HMG PKI.

3.7.1. The HMG PKI is implemented as a single hierarchy with the HMG Root CA at the top. A hierarchy is the simplest trust architecture[5] as only one trust point is needed to underpin all internal transactions. This simple architecture means that the management of the PKI is also simpler.

3.7.2. The HMG PKI Policy Management Authority (PMA) exercises control of the HMG PKI. The PMA is organised and chaired by the Office of the e-Envoy and one of its key tasks is to define a number of certificate policies that can be used in pan-governmental communications and for most communications with external partners. These HMG-wide certificate policies will be owned and maintained by the PMA.

3.7.3. The HMG Root CA sits at the top of the hierarchy and acts as the trust point for HMG-wide transactions, using the HMG-wide certificate policies. The HMG Root is offline and is only used to certify departmental CAs, and not end entities. This is

---

[5] Other architectures are possible such as directly cross-certified or bridge architectures. Discussion of these alternative architectures is outside the scope of this document.

done to minimise the vulnerabilities of the HMG Root CA and hence improve the security of the overall PKI.

3.7.4. Departments will operate (or have operated on their behalf) certification authorities underneath the HMG Root CA and may certify subordinate CAs or end entities directly. The HMG-wide certificate policies provide a good basis for e-business and e-government and in many cases these will be sufficient. Departments may, however, define their own certificate policies for their own internal use, subject to authorisation from the PMA[6]. If a department defines its own certificate policy, then the departmental CA (and not the HMG Root) will act as the trust point for all transactions that rely on certificates using this policy.

3.7.5. Each certificate that is issued within the HMG PKI will have at least one certificate policy that is applicable. Each applicable certificate policy will be identified explicitly within the certificate itself so it will be clear whether it is medium or high assurance. This will enable end entities (or applications on their behalf) to decide whether to trust the certificate based on the policy.

3.7.6. Figure 2 illustrates the overall structure for the HMG PKI using an example configuration.

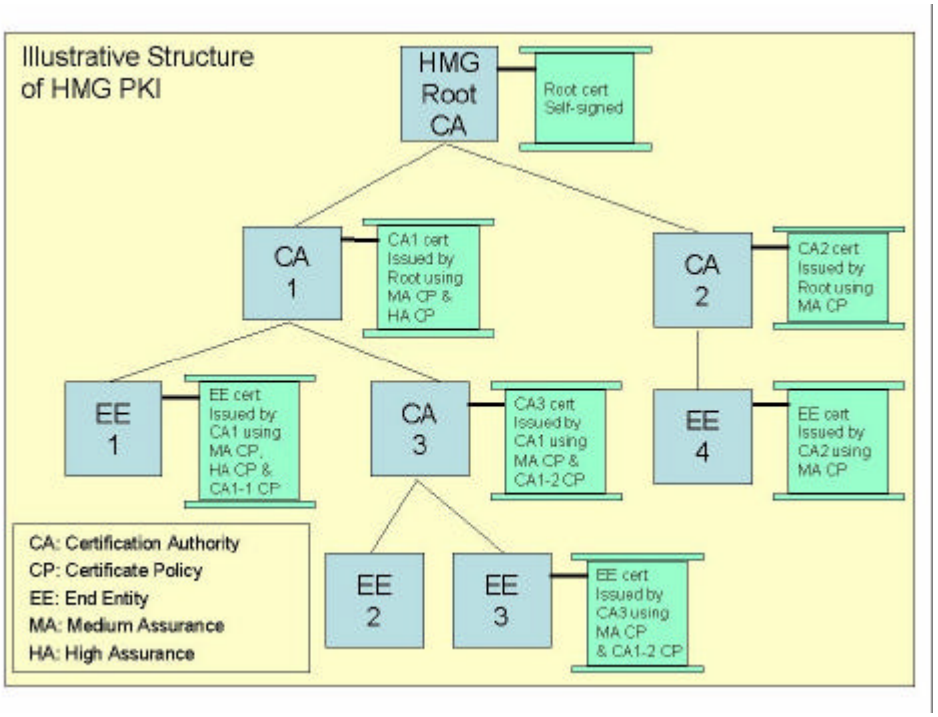

Figure 2: Overall structure for HMG PKI

3.7.7. In this example, two certificate policies have been defined with an HMG-wide scope:

a) a medium assurance (MA) signature certificate policy; and

b) a high assurance (HA) signature certificate policy.

3.7.8. As the HMG Root CA is at the top of the hierarchy, it has a self-signed certificate. This certificate does not need to state certificate policies explicitly – the Root is automatically trusted for all certificate policies.

---

6 Authorisation from the PMA is required to promote and facilitate re-use of HMG-wide certificate policies, where applicable.

3.7.9. All HMG PKI certificates (excluding the Root certificate) have been issued using the Medium Assurance (MA) certificate policy. CA 1, representing Department 1, operates a very secure CA in accordance with the HMG High Assurance (HA) certificate policy and has a certificate with both the MA and the HA policy defined. CA 2, representing Department 2 operates a secure CA that conforms to the HMG Medium Assurance (MA) certificate policy, but does not meet the requirements for the HA certificate policy. The CA 2 certificate only has the MA certificate policy defined.

3.7.10. Using this approach, interoperability at the pan-governmental and industry-facing level is achieved using the general medium assurance certificate policy (e.g. for secure messaging and e-commerce), while specific certificate policies can be supported at the departmental level if necessary. In *Figure 2* CA 1 has defined two departmental-level certificate policies: CA1-1 and CA1-2 – these two certificate policies are separate to the HMG-wide (MA and HA) policies and can be used internally within the department that operates CA 1.

3.8. What's the risk of not being part of the HMG PKI?

There may be problems of interoperability with the rest of government and resolving this may result in huge cost. There is also the important issue of appearing not to be 'joined-up'.

3.8.1. A major risk of not being part of the HMG PKI is that if a PKI solution is required and developed, it will not be interoperable with the rest of government and therefore will not enable the level of e-government and e-business services required.

3.8.2. There is also a high risk of 're-inventing the wheel', resulting in substantially increased timescales and resources. In addition, a non-HMG PKI solution will not capitalise on the trust relationships managed by the HMG PMA and will not present a 'joined-up' image of government to external parties.

3.9. How do we join the HMG PKI?

Contact the Policy Management Authority.

3.9.1. The first step is to contact the HMG PKI Policy Management Authority (PMA) outlining the requirements and current plans as applicable. The PMA can provide advice and guidance to facilitate the development of the necessary systems and procedures. All extensions to the HMG PKI through additional departmental CAs certified by the HMG PKI Root will need to be approved by the HMG PKI PMA.

Contact Details:-

Security Policy
Office of the e-Envoy
Stockley House
130 Wilton Road
London
SW1V 1LQ

Tel:- 020 7276 3105

Email:- security@e-envoy.gsi.gov.uk

A Abbreviations

This section describes the abbreviations used in this document.

CA	Certification Authority
CP	Certificate Policy
HMG	Her Majesty's Government
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority

Office of the e-Envoy, Stockley House, 130 Wilton Road, London, SW1V 1LQ

www.e-envoy.gov.uk