Australian Government
Department of Finance

Gatekeeper Public Key Infrastructure Framework Review

Discussion Paper

Ownership of intellectual property rights

Copyright Notice*

Third party copyright

Use of the Coat of Arms

Attribution

Feedback, Enquiries and Other Uses

The Department of Finance welcomes comments on this report. If you have feedback and enquiries about any aspect of the report or any questions about the CC licence or any other use of this document, please contact publications@finance.gov.au

Foreword

The Gatekeeper PKI Framework is a suite of policies, standards and procedures that guide how entities can prove their identities online (authenticate) when they attempt to access government services or systems. The Framework applies to individuals, organisations and computing components (e.g. devices or software).

Since its establishment in 1998, the Framework has played a vital role in strengthening trust in online transactions between government and the private sector. It has helped ensure the integrity, interoperability, and authenticity of systems and services that millions of Australians rely on.

The Framework has supported policy outcomes across multiple government agendas. However, as the digital landscape evolves with technologies like quantum computing and artificial intelligence becoming more prominent it is critical to assess whether the Framework remains fit-for-purpose. Industry and stakeholder feedback to date indicates that while the Framework's intent is sound, its current scope and requirements may be contributing to unnecessary complexity and inefficiencies. Both its design and implementation warrant review to ensure the Framework in its current or any future form, continues to be the most effective mechanism for enabling secure and adaptive digital engagement.

In response, the Government has initiated a formal review (the Review) to assess the Framework's future. This discussion paper seeks to stimulate public input by outlining current challenges, raising key questions, and presenting several policy options for consideration. It weighs the benefits of retaining the Framework against the case for reform or decommissioning it.

This is an invitation for broad and forward-looking dialogue that will inform the government position on the Framework's future. While this paper sets out the key areas for discussion, stakeholders are encouraged to provide submissions for consideration. I encourage all interested parties to put forward their views via gatekeeper.pki@finance.gov.au.

John Shepherd

Gatekeeper Competent Authority

Contents

Executive Summary

The Gatekeeper Public Key Infrastructure (PKI) Framework (the Framework), established in 1998, has served as a cornerstone for secure digital authentication across Australian Government and private sector interactions. As digital technologies and cybersecurity landscapes evolve, the Framework's relevance and effectiveness are being reassessed through a formal review led by the Department of Finance (Finance).

This paper outlines the scope, process, and policy context of the review, identifying key challenges such as low adoption, outdated references, and limited enforceability. Stakeholder input is sought on whether the Framework should be retained, reformed, or decommissioned. Key areas of focus include:

- **Policy Viability:** The Framework has at times been mandatory despite no legislative backing and unclear alignment with current cybersecurity directives such as the Protective Security Policy Framework (PSPF), Information Security Manual (ISM), and the *Digital ID Act 2024*.
- **Accreditation and Compliance:** The Gatekeeper Accreditation Program and Compliance Audit (GCAP) is intended to ensure high-assurance digital certificates, but enforcement mechanisms are limited. Accreditation relies on voluntary compliance and commercial incentives.
- **Strategic Alignment:** The Framework's alignment with national strategies like the 2023–2030 Australian Cyber Security Strategy is unclear, particularly in light of emerging technologies such as post-quantum cryptography (PQC), which will require significant updates to PKI systems.
- **International Comparisons:** Australia's approach compared with international models, including the EU's regulated eIDAS framework, the US Federal PKI ecosystem, and voluntary schemes in Canada and New Zealand. These comparisons highlight the diversity of governance models and raise questions about Australia's future role in PKI standard-setting.

Stakeholders are invited to provide input on:

1. What are the economic, security and productivity values and benefits of maintaining an Australian Government PKI framework?

2. The initial risk of coordination failure did not occur. Should the government consider relinquishing its current role?

If the Framework is retained:

3. Should a regulatory approach (which could include legislated monitoring powers, requirements and penalties for non-infringement) be considered to potentially replace the current Framework?

4. Should the Framework be reclassified as a best-practice policy to encourage an industry-led certification body?

5. Should the scope of a future PKI framework only apply to Government-to-Government transactions only?

6. Should a more limited update to the Framework be considered while the industry plan and implement their post-quantum cryptography transitioning?

Privacy Collection Notice

Your personal information is protected by law, including the *Privacy Act 1988*, and is collected by the Department of Finance (Finance) to evaluate submissions received via the email gatekeeper.pki@finance.gov.au in relation to the review of the Gatekeeper Public Key Infrastructure (PKI) Framework (the Framework) and to develop appropriate recommendations to Government on its whole of government information and communications technology. The personal information collected from submissions during the Framework consultation period may be disclosed to Finance employees, as well as other Australian Government agency employees where appropriate or necessary to report on industry preference when formulating recommendations to Government. Finance will not use or disclose the personal information collected in this consultation period for another purpose without your consent unless required or authorised by law.

Please note that you should not include anyone else's personal and sensitive information in your response and if you provide personal information relating to another individual, you must have sought their consent to provide their personal information for this purpose, and have shown them this Privacy Collection Notice.

Gatekeeper PKI Review

Terms of Reference

The Gatekeeper PKI Framework (The Framework), including its supporting Gatekeeper IRAP assessment guide, and Gatekeeper Compliance Audit Program (GCAP) were last updated in 2015. Since then, advancements have occurred across industry, including in the technologies, standards, and government policy.

The Government has requested that the Department of Finance (Finance) undertake a review of the Framework (the Review). The purpose of the Review is to better understand the viability of maintaining the Framework, and to support an informed decision on whether to update or decommission the Framework, including the Gatekeeper Accreditation Program. The Review will provide findings and recommendations to the Minister for Finance.

The Review will provide advice to Government on the following:

- whether the Framework has met the objectives set out in the original Gatekeeper Strategy in 1998;
- the viability of the Framework as a policy instrument
- the role of Government in setting nationally consistent standards and guidelines governing the use of PKI technology and regulatory options;
- potential changes and the effort required to update and maintain a revised Framework.

At this stage of the Review, Finance will not consider:

- Promoting or deprecating PKI as a form of technology for encryption and authentication.
- Mutual or cross-recognition of accreditation with other international frameworks as cross recognition of other accreditation frameworks can only be considered in a post-review context.

Process for the Review

The review will take place in three stages. A breakdown of each stage is as follows.

Stage 1: Governance arrangements for the Review

- The Review commenced with the establishment of governance arrangements
- The Review is overseen by a Board chaired by Finance and includes representatives from the Digital Transformation Agency (DTA) and the Australian Signals Directorate (ASD).

Stage 2: Open consultation on Discussion Paper

- A discussion paper (this paper) developed and released to seek responses on key policy questions;
- Finance will undertake targeted bilateral and multilateral engagement activities and receive written submissions from all interested parties;
- The discussion paper forms part of the Review and will outline and assess the arguments and policy options for maintaining the Framework and attempts to identify the economic, security and productivity benefits of maintaining an Australian PKI framework. Secondly, the paper considers the options available to the Government to address concerns about the Framework;
- Advice will be provided to the Minister summarising stakeholder feedback, including advice on the preferred option.

Stage 3: Final report and recommendations

- A second paper will be developed with stakeholders to facilitate further public consultations how preferred options will work and the associated transition arrangements;
- Depending on the consensus from Stage 2, this second paper may be accompanied by a detailed technical explainer detailing current and future state.

Considerations will be made on:

- opportunities for removing unnecessary and inefficient barriers to entry and competition;
- best practice developments internationally and in other industry sectors;
- reducing complexity; and
- eliminating duplication that providers are required to meet.

Policy Background and Setting

In the late 1990s the Framework established a national framework for the use of digital keys and the authentication of personnel and organisations that interact electronically with the Government. This was part of the Government's effort to foster business confidence of their online transactions and online identities.[1] To prevent coordination failure, the Government took steps in establishing itself as an example of better practice by adopting the Framework, National e-Authentication Framework (NeAF) and the Third-party Identity Services Assurance Framework to provide Trusted Online Identity.

These frameworks formed part of an overall identity and authentication policy setting to manage risk management across identity and authentication solutions (See Figure 2). Below is a brief outline of each Framework's purpose within the policy setting.

- The *National e-Authentication Framework (NeAF)* was developed to replace the Australia Government eAuthentication Framework. NeAF started as a suite of better practice guides for implementing digital authentication systems; it used a set of operating principles and relies on a risk-mitigation approach. It allocates the consequence of misuse into one of five categories, and then applies one of four levels of authentication to respond to that risk.[2]
- The *Gatekeeper Public Key Infrastructure Framework*, which is a whole-of-government accreditation program for the use of public key technology by Government agencies; and
- The *Third-Party Identity Services Assurance*, which is an accreditation framework for the use of commercially provided digital authentication services by Government agencies. These services include personal data vaults, digital mailboxes, data verification services and authentication services.

NeAF

NeAF was endorsed by the Council of Australian Governments (COAG) in 2008[3] and was made a mandatory framework for Government agencies from 2014.[4] It played a major role in the adoption of the Framework by providing directions for:

- electronic authentication of the identity of individuals and businesses including their agents or representatives; and
- electronic authentication of government websites.

Where appropriate NeAF referred to the use of high-assurance digital certificates provided by the Gatekeeper Framework for:

- electronic authentication of assertions other than identity;
- electronic authentication of transactions, addressing integrity and non-repudiation requirements;
- cross-organisational electronic authentication (e.g. between government agencies within or across jurisdictions, to include private and public sector initiatives);
- electronic authentication of non-human entities (machine to machine); and
- electronic authentication of individuals to support physical access controls.

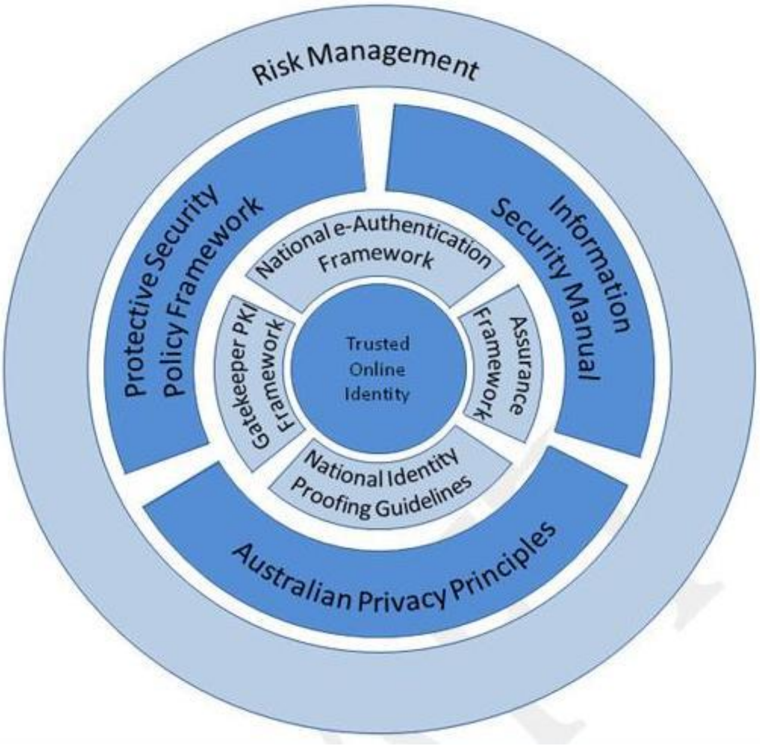
Risk Management
Protective Security Policy Framework
Information Security Manual
Australian Privacy Principles
National e-Authentication Framework
Gatekeeper PKI Framework
Assurance Framework
National Identity Proofing Guidelines
Trusted Online Identity

Figure 2: Identity and authentication Policy setting (2014)

The Third-Party Identity Services Assurance Framework (the Assurance Framework)

The Assurance Framework was developed as an initial Framework for government to manage and coordinate a mature market of various identity related solutions including:

- Digital mailbox providers
- Personal identity management or authentication providers
- Online verification providers
- Personal data management or data vaults providers

The Assurance Framework set out compliance criteria and accreditation requirements for these types of third-party providers who sought to offer services to government. The accreditation process facilitated accreditation status for their identity and verification solutions to a specific Level of Assurance (LoA).

The Assurance Framework and its accreditation process was endorsed on a whole-of-government basis by the Secretaries' ICT Governance Board (SIGB). The Assurance Framework was informed by and supported the National e-Authentication Framework (NeAF), the Gatekeeper PKI Framework, and the National Identity Security Strategy (NISS). It was predominantly developed to allow third party credentials to be utilised by agencies for their respective business needs while the Trusted Digital Identity Framework (TDIF) was being developed.

Trusted Digital Identity Framework (TDIF)

From 2018, the TDIF was developed to replace NeAF and the Assurance Framework.[5] TDIF evolved to focus on Digital Identity and business authorisation. Consequently, it did not fully replace all the aspects of electronic authentication assurance covered by NeAF.

TDIF was legislated as the *Digital ID Act 2024* (the Act) with its subordinate legislation commencing from 30 November 2024 to support the expansion of the Australian Government Digital ID System.

Has the Framework met the objectives set out in 1998?

The primary objective of the Framework is to encourage confidence in the online economy, and to ensure trust between all users at each level of transactions with government.[6]

As the adoption of the internet and electronic transactions is a global phenomenon, non-Gatekeeper accredited PKI providers have come to dominate the digital certificates market.

Australia has not been alone in developing a PKI framework to promote trust and assurance in electronic transactions. International standards and CA audit programs have been developed. Notably, the Web Trust Seal Program managed by the Chartered Professional Accountants of Canada (CPA) and the European Telecommunications Standards Institute (ETSI) offer their own structured approach for private sector and government run CAs to meet to be approved join various root CA programs including Microsoft Trusted Root Program[7] and Chrome Root Program[8].

The availability of these audit programs and the standardisation of protocols such as X509 for certificate format and communications raises the question on what value and benefits does the Framework offer to Australia. Furthermore, at the international level, several of Australia's strategic partners have an accreditation regime and only the European Union has a legislative framework (Appendix C).

The current depth and maturity of the PKI market clearly demonstrate that the initial risk of coordination failure (where market participants struggled to align on PKI standards) has been effectively addressed. This outcome reflects the success of earlier government interventions, such as the Framework, in fostering a coherent and trusted digital identity environment. However, the absence of coordination failure today does not, in itself, justify the continued application of the same policy instrument. Rather, it provides a timely opportunity to reassess the Government's role in this area and ensure that policy settings remain proportionate, contemporary, and aligned with the dynamics of a global integrated digital world.

Questions:

1. What are economic, security and productivity values and benefits of maintaining an Australian Government PKI framework?

2. The initial risk of coordination failure did not occur. Should the government consider relinquishing its current role?

The viability of the Framework as a policy instrument

There are currently eight Gatekeeper-accredited service providers across Government and the private sector. These service providers are responsible for issuing and managing thousands of Gatekeeper digital certificates and keys that are issued on behalf of a relying party to their customers that consume their services (see Appendix A).[9]

At the Commonwealth level, the Framework's use has been mandatory and there has been a history of established practices of agencies compliance (e.g. through NeAF). It should be noted that because Public Key Encryption (PKE) underpins the internet and digital communications, the bulk of digital certificates in use are not governed by the Framework (an overview of PKI and PKE can be found in Appendix B).

The status of the Framework as a mandatory whole of government policy has become unclear:

- The Framework is only considered as guidance under the DTA's Australian Government Architecture (AGA) resource, to support User Identity Management and Information Asset Security capabilities.
- The Framework is not designated as mandatory by a whole of government ICT policy.
- While the Framework is intended to be aligned with the Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM), there is no direction from the ISM and PSPF to comply with Framework.
- In the early 2000s, there was a Ministerial direction mandating the use of the Framework in electronic transactions with the Government. Since then, there has been no Ministerial direction.
- The requirement to use Gatekeeper PKI in the Australian Government Digital ID System was removed from TDIF version 1 onwards.
- While the use of Gatekeeper PKI is required for Electronic Lodgement Network Operators (ELNO) for electronic conveyancing. This is administered by states and territories.

The role of Government in setting nationally consistent standards and regulatory options

To provide high-assurance digital certificates required by NeAF, the Gatekeeper Accreditation Program assess and evaluate interested services providers (government or private sector entities) against the Framework requirements. Interested parties may become accredited as a Registration Authority, Certificate Authority or Validation Authority roles. See Appendix A for full list of accredited service providers.

For accreditation status to be approved, an initial evaluation must be conducted by an assessor from the InfoSec Registered Assessor Program (IRAP) facilitated by the Australian Signals Directorate (ASD) in alignment with the Gatekeeper PKI IRAP Guide. This evaluation mechanism was created in liaison with ASD (formerly Defence Signals Directorate) to mitigate the key risk profile identified in the original Strategy for service provider roles.

Accredited entities are required to undertake an annual audit under the GCAP. This is designed to ensure that accredited service providers continue to meet the minimum acceptable controls after their initial assessment.

Because Gatekeeper is policy and not a legislative requirement, this limits the levers available for enforcing compliance and the success of those levers largely depends on an entity's commercial incentives to remain accredited. Currently non-compliance is dealt with under the Framework through waivers or exemptions granted by the Gatekeeper Competent Authority (Finance). With limited coercive powers to enforce compliance, remediation activities rely on coordination between the provider and the Gatekeeper Competent Authority. Generally, removal of accreditation status is the only sanction available when a significant event of non-compliance is realised.

If the Framework is retained, stakeholders are invited to consider the following questions:

3. Should a regulatory approach which could include legislated monitoring powers, requirements and penalties for non-infringement be considered to potentially replace the current Framework? Or,

4. Should the Framework be reclassified as a best-practice policy to encourage an industry-led certification body? Under this option, the Government could play an initial coordination role before transferring the responsibility to a board of directors on which a lead agency could be a member. This will be co-designed in further details with interested stakeholders.

Potential changes and the effort required to update and maintain a revised Framework

The Framework currently refers to past versions of the Protective Security Policy Framework (PSPF), the Information Security Manual (ISM), and the National Identity Proofing Guidelines (NIPGs) which all have been extensively revised or in the process of review. In addition, the time between reviews of the Framework have highlighted that the Framework may no longer support the objectives of the 2023-2030 Australian Cyber Security Strategy. Below provides an overview of significant policy changes since the last update.

Protective Security Policy Framework

The Protective Security Policy Framework (PSPF) is an Australian Government initiative that commenced in 2010. The PSPF provides a set of guidelines and standards for managing security risks, ensuring compliance with legal and regulatory requirements, and fostering a culture of security within organisations. It has undergone several reforms, including in 2018[10], with new directives released in 2024[11].

The Framework refers to the PSPF version released in 2014. This presents several inconsistencies in the Framework's Gatekeeper Mandatory Security Requirements where the 2014 PSPF Mandatory Obligations do not map or exist in the current PSPF release (Gatekeeper 6 is an example of an obsolete obligation). Secondly, many of the Mandatory Requirements listed in the Framework have been consolidated into the revised PSPF.

Information Security Manual

The Information Security Manual (ISM) is published by ASD's Australian Cyber Security Centre (ACSC). It provides comprehensive guidelines and controls to help organisations protect their information and systems from cyber threats. The Framework references the ISM as a mandatory policy. The ISM is regularly updated to address emerging threats and technological changes, which poses the question as to if the ISM still has the relevant content to support the Framework which has remained static since 2015.

The 2023-2030 Australian Cyber Security Strategy

The Australian Cyber Security Strategy was released in 2023 and includes the Government's plan to build and develop six cyber shields to holistically defend Australia against cyber threats. An outdated PKI framework could undermine the cyber security shields objectives intended to protect critical infrastructure; trust in digital products and services; and continue to lead in shaping global rules and standards on the global stage the cyber security shields.[12]

While the strategy does not list PKI as a required technology, PKI does support large parts of the cyber eco-system and does provide several government agencies a mechanism to communicate securely by using Gatekeeper accredited certificates.

Digital Experience Policy

The Digital Experience Policy (DX Policy) came into effect from January 2025. It aims to transform how people and businesses interact with government digital services. Developed by the Digital Transformation Agency (DTA), the policy sets benchmarks for service quality and introduces four key standards: the Digital Service Standard, Digital Inclusion Standard, Digital Access Standard, and Digital Performance Standard. These standards promote user-centric design, inclusivity, accessibility, and continuous improvement. The policy applies across all government entities, including both corporate and non-corporate Commonwealth bodies, and covers both public-facing and staff-facing services. It aligns with the broader Data and Digital Government Strategy and strengthens the Investment Oversight Framework by integrating real-world data and user feedback into service planning and delivery.

The DX Policy addresses long-standing issues of fragmented and inconsistent digital experiences across government websites. It encourages agencies to design services that are adaptable, measurable, and easy to access, with a strong emphasis on leaving no one behind. Implementation is phased, beginning with new services in 2024 and expanding to existing services by 2026. Agencies are supported with toolkits, guidance, and compliance frameworks to ensure alignment and accountability. Ultimately, the policy seeks to deliver seamless, secure, and inclusive digital services.

Other policy regime changes to consider

The Framework has not been revised since 2015. Within the Framework's mandatory requirements, several other policy regimes have undergone changes.

The Framework also prescribes itself to align with international standards and audit programs delivered by the Canada Institute of Chartered Accountants WebTrust Program for Certificate Authorities and the European Telecommunications Standards Institute Electronic Signature and Infrastructure (ETSI) Policy requirements for Certification Authorities issuing public key certificates. Both these programs have been updated on a regular basis since 2015.

Table 1 shows the status of changed mandatory policy regimes referenced in the Framework.

Table 1: Identified status changes in Mandatory Policy Regimes

Mandatory Policy regimes

Policy regime referenced in the Gatekeeper Framework	Status changes since 2015	Latest version released	Agency/body responsible	Applicable to public or private sector
Protective Security Policy Framework (PSPF)	Reformed in 2018	2024	Department of Home Affairs	Both (Private sector where classified or sensitive government data is involved)
Information Security Manual (ISM)	Revised periodically	2025	Australian Signals Directorate (ASD)	Public sector
National Identity Proofing Guidelines (NIPGs)	Currently under review	2014	Attorney General Department	Guidance for both

Policy regime referenced in the Gatekeeper Framework	Status changes since 2015	Latest version released	Agency/body responsible	Applicable to public or private sector
Agency personnel security management guidelines	Consolidated into PSPF and archived	2011	Attorney General Department	Public sector
Australian Government personnel security management protocol	Consolidated into PSPF and archived	2014	Attorney General Department	Public Sector
Information Security Management Guidelines – Australian Government classification system	Consolidated into PSPF and archived	2014	Attorney General Department	Public Sector
Information Security management guidelines – management of aggregated information	Consolidated into PSPF and archived	2012	Attorney General Department	Public Sector
Information security management guidelines – Physical security of ICT equipment, systems and facilities	Consolidated into PSPF and archived	2012	Attorney General Department	Public Sector
Physical security management guidelines – Security zones and risk mitigation control measures13	Consolidated into PSPF and archived	2011	Attorney General Department	Public Sector
Protective security governance guidelines – business impact levels	Consolidated into PSPF and archived	2014	Attorney General Department	Public Sector

Policy regime referenced in the Gatekeeper Framework	Status changes since 2015	Latest version released	Agency/body responsible	Applicable to public or private sector
Securing government business – Protective security guidance for executives	Consolidated into PSPF and archived	2014	Attorney General Department	Public Sector
National Archives of Australia – Administrative Functions Disposal Authority	Reviewed, retired and replaced with ADFA Express Version 2 in 2025	2010	National Archives of Australia	Public Sector
ITU-T X.500 (10/12) Information technology – Open Systems Interconnect – The Directory: Overview of concepts, models and services	Superseded in 2019	2019	The International Telecommunication Union	Proposed standard, not mandated
National e-Authentication Framework	Decommissioned	2009	Department of Finance and De-Regulation	Public sector
Telecommunications Cabling Provider Rules 2000	Revoked and replaced	2014	Australian Communications Media Authority	Mandated for cabling operators and supervisors

Developments in Quantum Computing

Current cryptography standards will quickly become outdated due to advancements in quantum computing. These standards advise on which encryption algorithms provide the minimum-security strength requirement or key sizes to ensure any data transmitted over an insecure network is secure. Quantum computing is expected to dramatically increase computing power to the point where quantum computers will be able to break the security achieved using existing PKE algorithms.[14]

Due to these developments, ASD has issued advice in the Information Security Manual that PQC algorithms should be progressively adopted in Australia by 2030.[15] Therefore, Gatekeeper accredited service providers would be required to adopt these encryption algorithms and transition existing digital certificates and other PKI technologies if the Framework continues.

Transitioning to PQC will require PKI providers to upgrade their systems to issue digital certificates based on PQC standards and support end-user migration. This process will demand substantial investments of time and resources regardless of the outcome of the current review.

If the Framework is retained, stakeholders are invited to consider the following questions:

5. As the policy regimes in Table 1 are mostly applicable to the public sector, should the scope of a future PKI framework only apply to Government-to-Government transactions only?

6. Should a more limited update to the Framework be considered while the industry plan and implement their PQC transitioning? This could be followed by a more comprehensive update post 2030.

Glossary

Abbreviation	Meaning
AGA	Australian Government Architecture
API	Application Programming Interface
ASD	Australian Signals Directorate
CA	Certificate Authority
COAG	Council of Australian Governments
CPA	Chartered Professional Accountants of Canada
DTA	Digital Transformation Agency
ETSI	European Telecommunications Standards Institute
FTPS	File Transfer Protocol Secure
GCAP	Gatekeeper Compliance Audit Program
HTTPS	Hypertext Transfer Protocol Secure
IoT	Internet of Things
IRAP	InfoSec Registered Assessor Program
ISM	Informational Security Manual
M2M	Machine to Machine
NeAF	National E-Authentication Framework
PGP	Pretty Good Privacy
PKE	Public Key Encryption
PKI	Public Key Infrastructure
PQC	Post Quantum Computing
PSPF	Protective Security Policy Framework
RA	Registration Authority
S/MIME	Secure/Multipurpose Internet Mail Extensions
SFTP	Secure Shell File Transfer Protocol
SSL/TLS	Secure Sockets Layer and Transport Layer Security
VA	Validation Authority
VPN	Virtual Private Network

Appendices

Appendix A – Gatekeeper Accredited Service Providers and Government Relying Parties

Gatekeeper Service Provider[16]	Service type	Accreditation date
DigiCert (formally Symantec)	Certification and Registration Authority	September 2015
Cogito Group	Registration Authority, Certification Authority and Validation Authority	11 October 2021
Department of Defence	Certification and Registration Authority	17 May 2007
Department of Industry and Science	Validation Authority	6 January 2011
Medicare Australia	Certification Authority	29 June 2011
Verizon Australia	Certification Authority	16 February 2012
Australian Taxation Office	Certification Authority	30 April 2013
	Registration Authority	June 2019
Property Exchange Australia Limited	Certification Authority	1 October 2014
	Registration Authority	June 2019

Below are a few examples of where and how the Framework is used to support service delivery.

Australian Border Force (ABF)

The ABF Integrated Cargo System (ICS) is used for the management of imports and exports to and from Australia. This system requires high assurance in the authentication of users of the ICS so enrolled users can securely communicate with the ABF. To attain high assurance, the ICS is underpinned by gatekeeper accredited certificates. These certificates allow Individuals and businesses that are enrolled in the ICS to complete various processes, including to lodge import or export declarations via a web browser or Electronic Data Interchange (EDI) software.[17]

Australian Department of Defence

The Australian Department of Defence (Defence) has supported the use of the Framework since its inception by being accredited as a CA and Registration Authority since 2007 for PKI use within Defence.[18] Gatekeeper digital certificates are used in the electronic identification of entities as representatives or affiliates of Defence, and to provide authentication of defence personnel for secure online transactions within Australia and abroad with partner nations. Gatekeeper accreditation as an RA and CA continues to provide a vital foundation capability for Defence to achieve its identity management vision and is a critical component of defence technology systems.

In 2013, the Australian Defence Organisation (ADO) was added as a US Department of Defence (DoD) approved external PKI. Currently ADO has six approved Certificate Authorities (CAs), including two Root CAs – Australian Defence Public Root CA and Australian Defence Interoperability CA approved by the US DoD Federal PKI Authority.[19] Each Root CA and Gatekeeper compliant subordinate CA has gained approval by the Gatekeeper Competent Authority and the Defence Program Management Authority.

The Australian Defence Public Root CA is the top trust point in the Defence PKI system.[20] Both the Australian Defence Interoperability CA and the Australian Defence Public Root CA refer to the last updated version of the Gatekeeper Framework requirements for annual compliance purposes and to be trusted by internal and external relying parties.[21] Subsequently, the Australia Defence Public Root CA is also an approved CA participant for the Microsoft Trusted Root Program (2016 - 2036).[22]

Services Australia and Verizon Australia

Verizon manages and issues NASH PKI certificates on behalf of Services Australia. NASH PKI facilitates secure access and exchange of health information between registered healthcare providers. As part of NASH PKI, enrolled users of NASH can gain access to the My Health Record system, the Healthcare Identifiers Service, and the Healthcare Public Directory which allows registered persons to search and download Medicare Australia PKI and NASH PKI certificates.[23]

Transport Accident Commission (TAC)

The Transport Accident Commission (TAC) is a Victorian Government-owned organisation that utilises accredited gatekeeper digital certificates for secure electronic messaging between TAC and authorised users.[24] User can include TAC employees, contractors, service providers and other authorised people.[25]

Appendix B: Overview of Public Key Infrastructure

Public Key Infrastructure (PKI) is a governed structured approach to establish and organise the operational, technical and legal environment for issuing digital certificates. PKI frameworks are supported by policies, procedures, and technologies that establish the necessary infrastructure for managing the end-to-end lifecycle of private and public key pairs, also known as asymmetric encryption or public key encryption (PKE).

PKE is used widely software, hardware or other systems to:

- Secure communication over electronic networks (e.g. end-to-end encrypted messaging, secure API calls)
- Apply digital signatures for document- and code-signing (verifying sender identity and data integrity)
- Secure file-transfer protocols (SFTP, FTPS) to guarantee integrity/confidentiality in transit
- SSL/TLS (HTTPS) for web-traffic encryption, online transactions and login sessions
- Cloud-storage encryption (encrypting data at rest before or during upload)
- VPN tunnels (establishing encrypted links over public Internet)
- IoT device authentication and secure Machine to Machine (M2M) communication
- Blockchain/cryptocurrency transactions (transaction signing & identity proofing)
- Public Key Infrastructure (PKI) and certificate management (issuing, validating X.509 certificates)
- Encrypted email (S/MIME, PGP) to keep messages private on open networks

These are done through asymmetric encryption which requires two separate keys – one which is public and one which is private. Although different, the keys are mathematically linked in a manner which enables actions performed by one key to be verified with the other. See Figure 1 for a basic representation of how PKE could be used to secure a message.

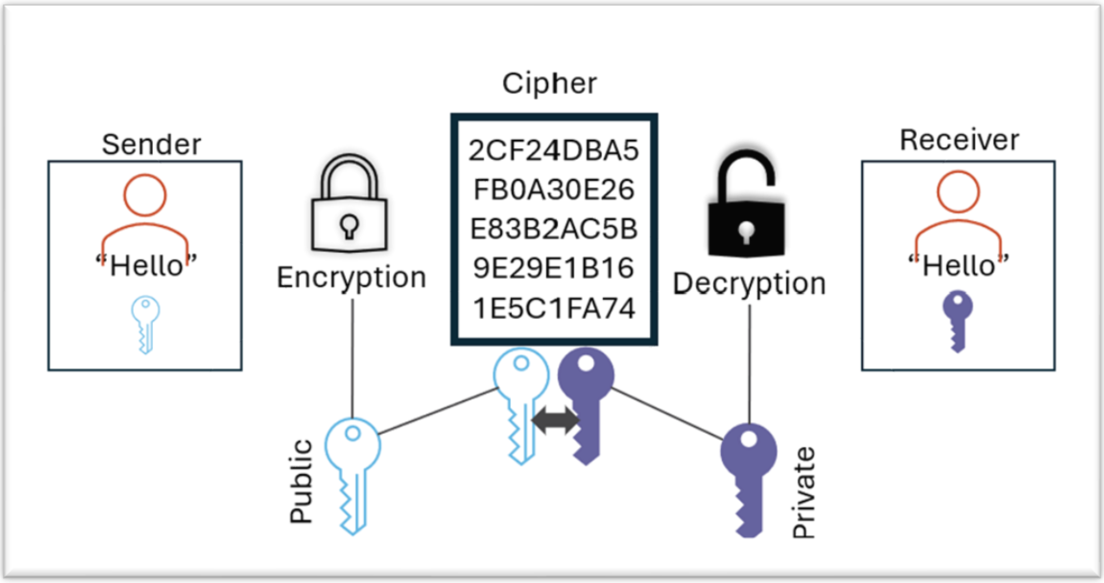

Figure 1: Basic representation of PKE or asymmetric encryption

In the above example a public key can be used to encrypt information or to verify a digital signature using an encryption cipher, whereas a private key can be used to decrypt information or to create a digital signature using a mathematically linked decryption cipher.

Digital certificates and digital signatures are the electronic representations of asymmetric encryption represented as an electronic file.

A digital certificate is a small electronic file that contains information identifying the person and/or an organisation. This is linked with the organisation identity with a digital resource for example, an email or software.

Certificate Authorities (CAs) are responsible for issuing digital certificates. Identity proofing of users and organisations is undertaken by Registration Authorities (RA). It is common for the RA and CA roles to be integrated into a single entity.

A digital certificate is used to create a digital signature. A digital signature contains a string of data created by hashing and encryption. A digital signature can be applied by software to show that digital content (email or digital document) has not been tampered with.

Appendix C: International PKE Implementation Overview

Even though the Framework is not mandated through any legal mechanism, it still acts as an Australian context specific approach to PKI implementation for government agencies. Other countries have their own varied approaches. Below covers PKE implementation designs in the European Union, United Kingdom, United States of America, Canada and New Zealand.

European Union

The European Union strictly regulates how European data, particularly government data and communications with their citizens are collected and managed. This has evolved into the need for standardisation of PKI certificates and electronic signatures across EU governments to ensure security, interoperability and trust. To facilitate this a European Parliament resolution was made in 2011.[26] Since then, considerable work has been done to develop regulation, directives and common standards that deliver this intention.

eIDAS Regulation

eIDAS was passed in 2014 to build and enhance trust, interoperability and security for online communication within the EU.[27] The eIDAS establishes the requirements for electronic signatures to have legal effect across member states. The term “electronic signature” in the EU includes three types of electronic signatures, which are simple electronic signatures, advanced electronic signature (AdES) and qualified electronic signatures (QES). AdES and QES are commonly facilitated by PKI technology through qualified certificates.[28]

The regulation also introduces the notions of qualified trust services (QTS) and qualified trust service provider (QTSP) that meet the high security trust services listed under the eIDAS regulation including QES. It also establishes the requirement for trusted lists of QTS and the use of a Trustmark. Non-compliance with eIDAS and associated directives attract penalties based on rules specific to each member state.

NIS & NIS2 Directives

The European Union’s Network and Information Security (NIS) Directive was established in 2016 with the aim of enhancing cybersecurity in the EU. In December 2022, the European Commission adopted a new version of the directive known as NIS2 that sets measures for a high common level of cybersecurity across the EU.[29]

A key component of NIS2 is that it mandates the use of end-to-end encryption at the union level as stated as[30]:

> *“(98) Where necessary, the use of encryption, in particular end-to-end encryption should be mandatory for providers of public electronic communications networks or of publicly available electronic communications services in accordance with the principles of security and privacy by default and by design for the purposes of this Directive.”*

Member states and critical or essential entities specified in the directive are “required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme”, which are provided by the European Union Agency for Cybersecurity (ENISA).[31]

ENISA QTSP/QTS Certification Scheme

All QTSP must undergo an independent Conformity Assessment and audit to facilitate mutual recognition of qualified certificates, eSignatures or eSeals across member states. The assessment and audit must be conducted by a national recognised accreditation body. These accreditation bodies are independent entities but accredited by the government and meet the requirements set out by the eIDAS regulation. For QTSP that have been assessed to meet their certification, re-assessment is required every 24 months, with some entities requiring a surveillance audit between full re-assessments.[32]

Dutch Government PKIoverheid Framework and EIDAS

The Dutch Government has implemented the PKIoverheid framework as part of its commitment to the European Commission's eIDAS regulation. PKIoverheid serves as a national infrastructure enabling secure and interoperable digital identities, allowing Dutch citizens and businesses to access public services both domestically and across borders using approved eID schemes like DigiD and eHerkenning. This framework ensures that digital interactions are also legally recognised throughout the European Economic Area.

At its core, PKIoverheid is underpinned by X.509 digital certificates, which are essential for enabling secure authentication, encryption, and digital signatures. These certificates are issued through a hierarchical trust model that includes root Certificate Authorities (CAs), intermediate CAs, and Trust Service Providers (TSPs). Each TSP must comply with stringent standards such as ETSI EN 319 411-1/2, ensuring that the certificates they issue meet both national and EU-level requirements (EIDAS) for trust and security. PKIoverheid chain of trust hierarchical structure is also audited to meet the WebTrust Seal program.[33]

United Kingdom

The UK does not legislate PKI minimum standards as the EU does for electronic transactions within their own borders. The UK instead has several mechanisms to provide high-level guidance and best practice standards for PKI for public and private sector service delivery.

tScheme

tScheme was formed in 2000 as an independent, not-for-profit organisation that provides approval to providers for their digital trust services. It is a self-regulating industry body that is market-led, meaning that their approval criteria maintain relevance as technology advances. Providers that hold a tScheme approval are eligible to indicate their services can be trusted using a tScheme Trustmark after proving compliance with the required standards.[34]

For PKI, there are several tScheme profiles that organisations must meet to gain approval by an independent tScheme assessor for the type of PKI service they want to provide. Depending on the sector and service provided, re-assessments and random audits are incorporated within the approval contracts provided by tScheme.[35]

National Cyber Security PKI Design (NCSC) Principles

The National Cybersecurity Centre (NCSC) was formed in 2016 as part of the UK Government Communications Headquarters (GCHQ) and aims to enhance the UK's cybersecurity posture.[36] One of its roles is to provide guidance and support to organisations on implementing secure systems, including PKI. The PKI Design Principles were developed as part of this mission and are used as best practice rather than a compliance and assessment mechanism.

There are currently eight key principles designed to address the complexities and challenges of modern PKI systems, ensuring organisations can provide secure, scalable, and interoperable PKI services. The key principles cover aspects such as trust model definition, certificate policies, key management, security controls, audit and compliance, interoperability, scalability and performance, and incident response.[37]

UK eIDAS Regulation

The exception to the UK's self-regulating system referred to above is where cross-border transactions are required with the EU. In response to this, the UK eIDAS regulates cross-border electronic transactions with the EU through laws made post-Brexit. This enables UK organisations to meet the stringent standards that exist in the EU within their own eIDAS regulation. It establishes a framework for digital identity and authentication and sets standards for electronic signatures and trust services.[38] tScheme is a recognised body within the EU to provide a voluntary accreditation scheme for UK trust service providers wanting to operate internationally.[39] For Trusted Service Providers that breach the UK eIDAS, a penalty notice is imposed by the Information Commissioner's Office (ICO).[40]

United States of America

PKI is a voluntary capability for US government agencies to participate in and is managed by the General Services Administration (GSA) office which facilitates the Federal Identity, Credential and Access Management (FICAM) Program. This program is designed to support federal agencies that choose to utilise PKI as part of their identity management operations. The GSA Office of the Chief Information Officer (OCIO) is responsible for security authorisations and continuous monitoring for commercially operated PKI shared service providers and acts as the centralised authority for identity management. This includes oversight activities for entities participating in the Federal Public Key Infrastructure (FPKI or Federal PKI) ecosystem.

The Federal PKI Ecosystem

The FPKI ecosystem is made up of US federal, state, local, tribal, territorial, and international governments, as well as commercial organisations that work together to provide services for the benefit of the federal government.[41] Within the FPKI ecosystem, the Federal Common Policy Certificate Authority (FPKI CA) G2 sits at the centre of the PKI network and is managed by Entrust Managed Services CA Shared Service Provider.[42]

Entities that participate as a PKI certification authority within the FPKI must have been certified by the Federal PKI Policy Authority (FPKIPA) and undergo annual audits by an independent auditor that detail their continued integrity and maintenance of their operating environment against the common policy.[43]

The FPKIPA acts as a central authority to enable an interoperable environment for entities or organisations through cross-certification policies. Interoperability is enabled by the Federal Bridge CA (FBCA) which was originally a prototype designed by Entrust Managed Services back in 2002.[44] The FPKIPA operates a cross-certification approval framework for Bridge

CAs such as the Australian Defence Organisation (ADO) PKI.[45] The FPKIPA is also responsible for the management of non-compliance to the common policy where identified.[46]

Canada

The Canadian Government allows departments to choose whether they utilise PKI as part of their identity and access management operational capability. Where PKI is chosen, departments must engage with the government's own Internal Credential Management (ICM) Public Key Infrastructure (PKI) services. This service provides PKI that meet the common PKI policies issued and managed by the Treasury Board of Canada Secretariat (TBS). For any PKI that is not provided by the ICM, a business case must be provided to the Office of Information Commission (ICIO) with approval sought. Interoperability between separate PKI systems in different departments or external entities must cross-certify through the Canadian Federal PKI Bridge (CFPB).[47]

New Zealand

The New Zealand government operates a voluntary, All-of-Government (AOG) PKI service to interested departments and agencies.[48] It is managed by the Department of Internal Affairs (DIA) in partnership with the Cogito Group. The Cogito Group is the only provider that offers PKIaaS and is aligned with the New Zealand Government PKI Framework.[49] This framework is outlined in the X.509 Certification Practice Statement for the New Zealand Government Public Key Infrastructure (PKI) that creates a consistent approach for PKI operational deployment across government and relying parties.[50] There is no formal compliance or assessment scheme for PKI providers in New Zealand.

Table 2: Governance comparison

Governance Comparison

Country	Regulated (Y/N)	Government run Accreditation Scheme (Y/N)	Annual Audits (Government or private sector auditors)
Australia	N	Y	Y
New Zealand	N	N	N
European Union	Y (For Member state governments and critical sectors)	Y	Y
United States	N	Y	Y
United Kingdom	N (except UK eIDAS)	N	N
Canada	N	N	N

References

[1] Trove, National e-Authentication Framework (NeAF) [PDF], 17 Feb 2014 – www.finance.gov.au/files/2012/04/NeAFFramework.pdf - Trove, 17th of February 2014, accessed 27

[2] Office of Government Information Technology, Gatekeeper Strategy [PDF], 1998, accessed 25 June 2025

[3] Department of Home Affairs, COAG - Report to the Council of Australian Governments: A Review of the National Identity Security Strategy [PDF], 2012, Accessed 5 July 2025.

[4] Trove, National e-Authentication Framework (NeAF) [PDF], 17 Feb 2014 - www.finance.gov.au/files/2012/04/NeAFFramework.pdf - Trove, 17th of February 2014, accessed 27 July 2025

[5] Security Brief, Australia's digital ID framework now one step closer reality [website], 2018, accessed 5 July 2024

[6] Boyle, Kate --- "An Introduction to Gatekeeper: The Government's Public Key Infrastructure" [2000] JlLawInfoSci 3; (2000-2001) 11(1) Journal of Law, Information and Science 38

[7] Microsoft, Program Requirements - Microsoft Trusted Root Program, Section 2 – Audit requirements, 29 October 2024, accessed 8 December 2024

[8] The Chromium Project, Chrome Root Program Policy, V 1.5, section 3 – Modern Infrastructures, 16 January 2024, accessed 8 December 2024

[9] Department of Finance, Gatekeeper Public Key Infrastructure Framework [website], 27 August 2024, accessed 5 November 2024

[10] Australian Government Department of Home Affairs, The new Protective Security Policy Framework commenced on 1 October 2018 [website], 1 October 2018, accessed 18 November 2024

[11] Australian Government Department of Home Affairs, PSPF Direction Update – July 2024 [website], 8 July 2024, accessed 18 November 2024

[12] Department of Home Affairs, 2023-2030 Australian Cyber Security Strategy, November 2023, accessed January 2025

[13] Attorney-General's Department, Physical security management guidelines [PDF], 2011, accessed 27 June 2025

[14] KPMG, Quantum is coming — and bringing new cybersecurity threats with it [website], April 2024, accessed 5 November 2024

[15] Australian Signals Directorate (ASD), 22. ISM - Guidelines for Cryptography (December 2024).pdf, December 2024, accessed February 2025

[16] Department of Finance, Gatekeeper Public Key Infrastructure Framework [website], 27 August 2024, accessed 1 July 2025

[17] DigiCert, Gatekeeper: Gatekeeper for Customs Users, Gatekeeper portal, n.d., accessed 28 November 2024

[18] Digital Transformation Agency (DTA), Gatekeeper Public Key Infrastructure Framework, V3.1 December 2015

[19] United States Department of Defence (US DoD), DoD Approved External PKIs Master Document [PDF], V 11.2 p.2 21 October 2024

[20] Australian Government Defence, X.509 Certificate Policy for the Australia Department of Defence Public Root Certificate Authority and Subordinate Certificate Authorities [PDF], V6.1 p. 9 December 2024

[21] Australian Government Defence, X.509 Certification Practice Statement for the Australian Department of Defence, V 11.1 p.11 & p.39 December 2024

[22] Microsoft, Included CA Certificate List [website], accessed 6 January 2025

[23] Australian Government Services Australia, NASH PKI [website], n.d., accessed 17 December 2024

[24] Transport Accident Commission (TAC) Victoria, Our organisation - TAC - Transport Accident Commission [website] About TAC, accessed February 2025

[25] DigiCert, Gatekeeper: Gatekeeper for TAC Users [website], Gatekeeper portal, n.d., accessed 17 December 2024

[26] European Parliament, Completing the internal market for e-commerce European Parliament resolution 21 September 2010 on completing the internal market for e-commerce, Resolution (2010/2012(INI)), *Office Journal of the European Union,* accessed 11 December 2024

[27] European Parliament, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Regulation L. 257|73, *Office Journal of the European Union*, accessed 11 December 2024
[28] European Commission, What is eSignature, [website], n.d., accessed 11 December 2024
[29] European Commission, New rules to boost cybersecurity of EU's critical entities [press release], 17 October 2024, accessed 11 December 2024
[30] European Parliament, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (NIS2 Directive), L 333/80(98), 27 December 2022, *Office Journal of European Union,* accessed 11 December 2024
[31] European Parliament, NIS2 Directive, L 333/80 Article 24, 27 December 2022, *Office Journal of European Union,* accessed 11 December 2024
[32] European Union Agency for Cybersecurity, Conformity Assessments of QTPS, ENISA, March 2020, p.14, accessed 11 December 2024
[33] Logius, PKILoverheid [website], n.d., Accessed 25 June 2025
[34] tScheme Trust Services, About Us | tScheme [website], n.d., accessed 5 November 2024
[35] tScheme Trust Services, Approval Profiles | tScheme [website], n.d., accessed 6 November 2024
[36] National Cyber Security Centre (NCSC), What we do - NCSC.GOV.UK [website], n.d., accessed 6 November 2024
[37] NCSC, Design and build a privately hosted Public Key Infrastructure, Guidance, n.d., p.9, accessed 6 November 2024
[38] Informational Commissioner's Office (ICO), What is the eIDAS Regulation? ICO, n.d., accessed 6 November 2024
[39] tScheme Trust Services, About Us | tScheme [website], n.d., accessed 5 November 2024
[40] Informational Commissioner's Office (ICO), Enforcement, ICO, n.d., accessed 6 November 2024
[41] IDManagement, Federal Public Key Infrastructure 101, United States Government [website], n.d., accessed 1 November 2024
[42] IDManagement, FPKI Ecosystem Changes, United Stated Government [website], n.d., accessed 1 November 2024
[43] ID Management, Annual Review Requirements [PDF], United States Government, V 2.0, 10 September 2024, accessed 24 December 2024
[44] Route Fifty, Federal bridge opens to two-way traffic - Route Fifty [website], May 2002, accessed February 2025
[45] US Department of Defense (DoD), DoD Approved External PKIs, Australian Defence Organisation (ADO) PKI, p.31, October 2024, accessed February 2025
[46] Federal Public Key Infrastructure Policy Authority (FPKIPA) Non-Compliance Management Framework for the FPKI [PDF], FPKIPA, V 1.0.1, 6 January 2024, accessed 24 December 2024
[47] Government of Canada, Public Key Infrastructure Configuration Requirements [website], n.d., accessed 19 December 2024
[48] New Zealand Government, New Zealand Government Public Key Infrastructure [website], n.d., accessed 20 December 2024
[49] Cogito Group, Public Key Infrastructure as a Service – Fact Sheet [PDF], March 2023, accessed 20 December 2024
[50] New Zealand Government, X.509 Certification Practice Statement (CPS) for the New Zealand Government Public Key Infrastructure Root and Shared Certificate Authority, X.509 CPS [PDF], Department of Internal Affairs, V 1.3, 11 December 2020, accessed 20 December 2024