		CertifyID Standard	CertifyID Advanced	CertifyID Qualified
General Description of the Class		It is useful for general purpose e-ID security that needs more than a simple login password system, and for assuring basic email integrity and confidentiality.	These e-IDs can be used for applications that require a reasonably high level of security. Increased identity assurance, with email integrity and confidentiality, PKI strong authenticaiton, enhanced interoperability an security with IDM systems, mail servers, secure web sites, encryption file system and smart card logon functionalities.	This class of e-IDs are issued as high security and intended to comply with specific legal and technical requirements adopted by local law and/or regulations. These e-IDs may be part of a national ID system or IDs issued to an individual for specific transactional usage. Provides a high level of identity assurance and confidentiality. Financial applications, contracts, agreements. Expanded functionality beyond advanced level.
PKI Disclosure		Enhances security moderately by assuring that the email address in subscriber certificates is accessible by the certificate subscriber. A CA on customer premises is restricted to only issue certificates containing email addresses within the domain owned by the organization. For certificates issued to real persons, businesses are responsible, but not required, to validate user identities based on organizational records, derived from in-person validation of presented credentials.	Enables individual certificates to be issued containing domain names belonging to the organisation's registered domains. Enables organizational certificates, especially SSL certificates, to be issued that belong to the organisation's registered domains. Relying parties can authenticate organizational identities, such as web sites. Provides increased assurance. For real persons, the organization is contractually obligated and required to verify individual's identity against organizational records, or trusted third party databases such as credit bureaus, or national registrars.	Provides extremely high trust assurance. Uses enhanced procedures such as face-to-face verification, which requires physical subscriber presence and presentation of identity credentials before certificate issuance, or other similar procedures. Enables more features than the advanced level.
End User Identity Validation	***ID data verified***	Basic data is verified such as the email address; or in the case of an organisation ownership of the domain names in the certificate, with responsibility to verify the individual entities to whom certificates are issued.	Personal identity data such as name, date of birth, nationality, etc. Legal entities are required to provide relevant official documentation. Verification of device or other type of entity or object is done with substantially equivalent data. Obligation to verify the identity of real persons.	Personal identity data such as name, date of birth, nationality, etc. Legal entities are required to provide relevant official documentation. Verification of device or other type of entity or object is done with substantially equivalent data.If local law compliance intended, then local law requirements apply and override.

		CertifyID Standard	CertifyID Advanced	CertifyID Qualified
	Method of verification	Bounce back email verification procedure proving access to the email account is accepted. Database (such as existing HR, or IDM) of organisation, with details of organisation's users. Commonly accepted business methods of identity verification.	May be done through database of identity data that is well-maintained and was created based on face to face or direct verification using official ID documents.	Face to face or direct verification but may be done through database of identity data that is well-maintained and was created based on face to face or direct verification using primary ID documents. If local law compliance intended, then local law requirements apply and override.
	Entities authorised to verify	The entity purchasing and managing the e-ID system under contract with WISeKey. Authorised internal entity (e.g. human resources dept.) or external entity who is legally bound to comply with the verification procedures. (Conditions are typically incorporated within purchase contract.)	Authorised internal entity (e.g. human resources dept.) or external entity who is legally bound to comply with the verification procedures. The entity purchasing and managing the e-ID system under contract with WISeKey. (Conditions are typically incorporated within purchase contract.)	Authorised internal entity (e.g. human resources dept.) or external entity who is legally bound to comply with the verification procedures. The entity purchasing and managing the e-ID system under contract with WISeKey. If local law compliance intended, then local law requirements apply and override.
e-ID Security	***Key Generation***	Key generation can take place on any approved device, and systems. Approved devices systems include most operating systems, browsers, smartcards and mobile devices.	Key generation can take place on any approved device, and systems. Approved devices systems include most operating systems, browsers, smartcards and mobile devices. Non-repudiable key pairs (as indicated in certificate policy) must not be exportable or escrowed.	Key generation for signature key pairs must take place on a secure device, Such as a smartcard or USB token, that is preferably accredited to FIPS-140-L1 or higher. Key generation for authentication and encryption can take place in non-FIPS accredited devices.
	Type of Token	Any approved storage device can be used for key generation and storage.	Any approved storage device can be used for key generation. Non-repudiable signature key pairs should not be exportable.	FIPS-140-L1 or higher. If local law compliance intended, then local law requirements apply and override.
	Validity Data Updates (CRL)	At least once per day.	At least once per day.	CRL must be published at least once per day. If local law compliance intended, then local law requirements apply and override.

		CertifyID Standard	CertifyID Advanced	CertifyID Qualified
	Key Escrow?	Recommended only for encryption keys.	Prohibited for signing keys. Only allowed for encryption keys.	Key escrow is permitted only for encryption key pairs, that do not have non-repudiable signature attribute set. If local law compliance intended, then local law requirements apply and override.
	Method of Renewal	Same as initial method of verification. Can use secret or authentication attributes established during initial verification, including existing key pair.	Same as initial method of verification. Can use secret or authentication attributes established during initial verification, including existing key pair.	Authentication via existing key/pair certificate; authentication over a secure channel using a known secret; in presence authentication. If local law compliance intended, then local law requirements apply and override.
	Who can suspend or revoke?	User can suspend or revoke after authentication; RA can suspend or revoke.	User can suspend or revoke after authentication; RA can suspend or revoke.	User can suspend or revoke after authentication; RA can suspend or revoke. If local law compliance intended, then local law requirements apply and override.
CA Auditing	***CA Identity & Authority Verification***	Generally a legal entity. Multiple verification procedures to ensure identity, domain name or other relevant data ownership and internal authority. Generally these include direct verification.	Generally a legal entity. Multiple verification procedures to ensure identity, domain name or other relevant data ownership and internal authority. Generally these include direct verification.	Comprehensive verification that includes direct verification and site visits. If local law compliance intended, then local law requirements apply and override.
	Who Audits?	WISeKey or a designated third party audits. Self-audits must also be conducted by entity managing the e-ID system.	WISeKey or a designated third party. Self-audits must also be conducted by entity managing the e-ID system.	WISeKey and an independent auditor certified by WISeKey or the OISTE Foundation regarding compliance with WISeKey's practices and policies. If local law compliance intended, then local law requirements apply and override.
	What is audited?	Compliance with all of the Class requirements	Compliance with all of the Class requirements	Compliance with all of the Class requirements. If local law compliance intended, then local law requirements apply and override.

		CertifyID Standard	CertifyID Advanced	CertifyID Qualified
	When is it audited?	Self audits are required and a site audit may be requested at any time. Third party audits (by WISeKey or designated entity) are required annually, or more frequently if prescribed by independent auditor. Technical audit controls and reporting is required on the CA system, and the CA certificate will be automatically suspended and subsequently revoked if the audit report is not provided with required frequency.	Self audits are required and a site audit may be requested at any time. Third party audits (by WISeKey or designated entity) are required annually, or more frequently if prescribed by independent auditor. Technical audit controls and reporting is required on the CA system, and the CA certificate will be automatically suspended and subsequently revoked if the audit report is not provided with required frequency.	Self audits are required and may be requested at any time. Third party audits are required annually, or more frequently if prescribed by independent auditor. Technical audit controls and reporting is required on the CA system, and the CA certificate will be automatically suspended and subsequently revoked if auditing report is not provided with required frequency.
Certification Services Security	***Physical Security***	RA access and authentication is ensured by strong authentication and encrypted network channels. RA and CA records and archives must be securely stored and protected. The CA must be protected with at least 2 levels of access (this can be locked room or specific safe).	RA access and authentication is ensured by strong authentication and encrypted network channels. RA and CA records and archives must be securely stored and protected. CA must be protected by at least 2 levels of access control before access to e-ID system server room. Accumulated access controls over 2 levels should be at least 2 factors (e.g. key, card, biometrics, password).	At least 3 levels of access control before access to e-ID system server room. Accumulated access controls over 3 levels should be at least 3 factors (e.g. key, card, biometrics, password). Other similar control mechanisms applicable to other areas.
	e-ID System Operator Personnel Security	Background checks on all personnel with access authority or with ID verification authority. Internal authorisation letter required. Information sent to authorising entity on importance of function.	Minimum background checks on all personnel with access authority or with ID verification authority. Checks should include identity, references, education verification, financial credit report & criminal history. Internal authorisation approval is required.	Minimum background checks on all personnel with access authority or with ID verification authority. Checks should be periodic and include identity, references, education veriication, criminal and credit history. Internal authorisation approval is required.

		CertifyID Standard	CertifyID Advanced	CertifyID Qualified
	Network Security	Firewalls, intrusion detection and prevention systems are employed where necessary to segregate and protect the Infrastructure network from other network elements, and prevent intrusion attempts. Antivirus and antispyware monitoring tools must be implemented.	Firewalls, intrusion detection and prevention systems are employed where necessary to segregate and protect the Infrastructure network from other network elements, and prevent intrusion attempts. Antivirus and antispyware monitoring tools must be implemented.	Firewalls, intrusion detection and prevention systems are employed where necessary to segregate and protect the Infrastructure network from other network elements, and prevent intrusion attempts. Antivirus and antispyware monitoring tools must be implemented.
	CA Key Generation, Size, Storage & Archival	CA key generation occurs within a secure cryptographic device meeting the appropriate ISO 15782-1/FIPS 140-2/ANSI X9.66 level requirement as disclosed in the Operator's business practices. HSM FIPS 140-2 Level 2. CA Private key recovery is recommended.	CA key generation occurs within a secure cryptographic device meeting the appropriate ISO 15782-1/FIPS 140-2/ANSI X9.66 level requirement as disclosed in the Operator's business practices. HSM FIPS 140-2 Level 2. CA Private key recovery is recommended.	CA key generation occurs within a secure cryptographic device meeting the appropriate ISO 15782-1/FIPS 140-2/ANSI X9.66 level requirement as disclosed in the Operator's business practices. HSM FIPS 140-2 Level 3. CA Private Key Recovery is required.
	e-ID System Key Usage Limitations	Client authentication, Secure Email (Digital Signature and Encryption), Key Archival, Delegated OCSP Signer	Client authentication, Secure Email (Digital Signature and Encryption), Certification Replication with Mail Servers, SSL Certificates (Server Authentication), Windows Smartcard Logon, File Encryption, Key Archival, Delegated OCSP Signer	Customisable according to client's needs. Defined on a per project basis. If local law compliance intended, then local law requirements apply and override.
	Domain Name Limitations	e-IDs can only be issued containing domain names owned by the entity and listed on the CA certificate.	e-IDs can only be issued containing domain names owned by the entity and listed on the CA certificate. Exceptions may be made for certain entitities with extra controls in place, who meet the audit criteria.	None.
	CA Certificate Directory / OCSP Service	Optional	Optional	Optional. If local law compliance intended, then local law requirements apply and override.

		CertifyID Standard	CertifyID Advanced	CertifyID Qualified
	CA System Changes	Prohibited without authorisation from WISeKey. Failure to acceed to a spot audit, deliver audit reports, or otherwise meet security requirements may result in immediate suspension or revocation of CA certificate.	Prohibited without authorisation from WISeKey. Failure to acceed to a spot audit, deliver audit reports, or otherwise meet security requirements may result in immediate suspension or revocation of CA certificate.	Strict testing and change management policies are adopted and required to be complied with. Operator implements monitoring and configuration control policies for the Service Infrastructure systems where necessary. If local law compliance intended, then local law requirements apply and override.
	Record Archival	Minimum 5 years.	Minimum 10+E25 years.	All records collected directly by Opeartor and Registration Authorities providing their services to the Operator concerning the operation of its certification services are archived and are retained for a minimum period of ten (10) years.
	Disaster Recovery	Disaster recovery policy required that ensures: availability of CRL within at least 1 week of disaster or CA revocation and decomissioning. Required minimal non-stringent : Ability to recover CA key in case of loss, through a backup. Ability to recover database in case of corruption.	Disaster recovery policy required that ensures availability of CRL within 1 week of disaster, or CA revocation and decommissioning. Revocation capabilities required operational within 2 weeks of disaster, or CA revocation and decommissioning. Required minimal non-stringent : Ability to recover CA key in case of loss, through a backup. Ability to recover database in case of corruption.	Disaster recovery policy required that ensures ongoing availability of the e-ID system within 24 hours of disaster. f local law compliance intended, then local law requirements apply and override.
	CA Termination	Any time without formal notice.	Requires formal prior notice of at least 1 month.	Requires formal prior notice of at least 6 months. If local law compliance intended, then local law requirements apply and override.

		CertifyID Standard	CertifyID Advanced	CertifyID Qualified
Liability	***Who is Liable?***	Unless resulting from WISeKey non-compliance with CPS, the entity managing the e-ID system or its users.	Unless resulting from WISeKey non-compliance with CPS, the entity managing the e-ID system or its users.	Unless resulting from WISeKey non-compliance with CPS, the entity managing the e-ID system or its users. If local law compliance intended, then local law requirements apply and override.
	Financial Responsibility	Whatever the entity managing the e-ID system indicates or as determined by law.	Whatever the entity managing the e-ID system indicates or as determined by law.	Whatever the entity managing the e-ID system indicates or as determined by law. If local law compliance intended, then local law requirements apply and override.