
# Future directions of the AusCERT Certificate Service

# QV Advanced Plus certificates

- Purpose
  - Digital signatures – non-repudiation, authenticity and integrity
  - Encryption - confidentiality
  - Client authentication – access control, including smart cards
- High assurance
  - Applicant must comply with identity verification and documentation requirements and submit these to QuoVadis
  - Auditable to ensure compliance
- Can only be issued on to a secure signature creation device (token) to  protect the private key
- Legally binding in some jurisdictions – accepted as equivalent of a witnessed pen-ink signature
  - European Telecommunications Standards Institute and Electronic Signatures Directive (1999/93/EC)
- QuoVadis (issuing CA) is in the Adobe Approved Trust List
- Long term validation
  - the ability of a signed document to stay valid many years or even decades after it was signed.

# Secure Signature Creation Device

- QV Advanced Plus certificate can only be issued onto a SSCD
- Properties of cryptographic USB token
  - Various models/manufacturers, eg, SafeNet eToken 5100
  - FIPS and Common Criteria (EAL4+) rated cryptographic devices
  - Used to generate and securely store PKI certificates and private keys
    - Private key can’t be exported
  - To authenticate, user must have the token and the password to access it
  - Tamper evident casing
  - Brute force attack proof
    - If a password is entered incorrectly 10 times in a row the token is disabled. The token can then be re-initialised (wiped clean) and new certificate can then be installed.

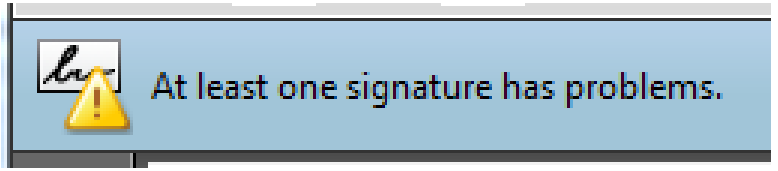
# PDF signing certificates - manual

- QV Advanced Plus certificate are issued to a person (certificate holder)
- Uses for manual signing
  - non-repudiation, authenticity and integrity
  - contract signing – multiple signatures possible
  - publicly distributing authorised versions of official documents
  - signing forms
- Revocation
  - Signatures are automatically timestamped by Adobe when the signature is created
    - Signature remains valid even after the certificate has expired or the certificate revoked

# What is required to create and view PDF digital signatures?

- Sign
  - Adobe Reader X or above (or Acrobat Standard or Pro)
  - A digital certificate
    - to avoid the authenticity check failing the Issuing CA (ICA) must be in the Adobe Approved Trust List (AATL)

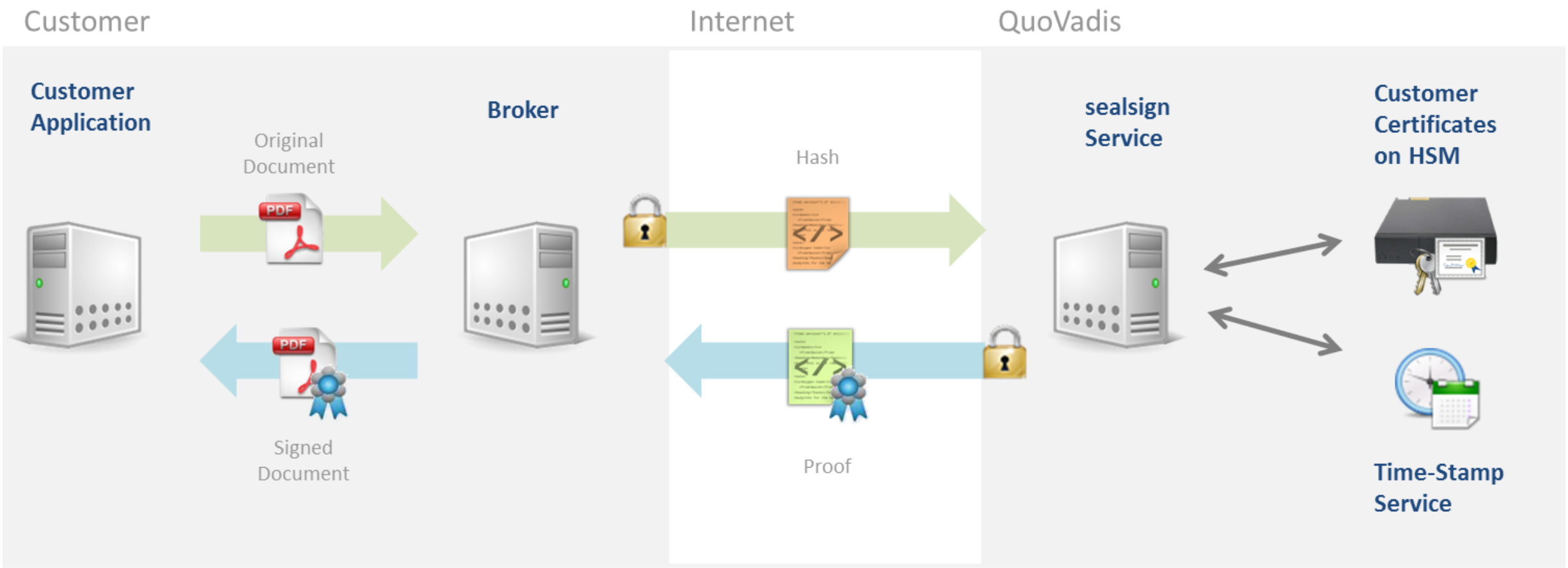
- View and verify
  - Internet access for initial view of the PDF
    - If a user opens a PDF that contains a signature, Adobe Reader checks for updates to its AATL. If not already in the local AATL, the ICA certificate is downloaded and installed for future reference.
  - Adobe Reader X or above
    - Or any source PDF software that conforms with the PDF Advanced Electronic Signatures standard (European Telecommunications Standards Institute (ETSI) TS 102.778).



# Bulk signing services

- Designed for bulk signing of documents, eg student transcripts
- Cloud based service provided by QuoVadis
- Minimal integration required with existing systems
  - Server based – no human interaction
- Certificate can be issued to a person or to the organisation
- The document is not sent to QV, only a hash of the document is sent – confidentiality is protected
- The  hash and timestamp are signed and applied to the document
- May be used for PDFs and other formats
- Can use embedded or visible signatures

# Bulk signing service



# Why digitally sign student academic transcripts?

- Approximately 1.1 million university students and about 350k students graduate PA
- 25% foreign students
- Many thousands of copies of requests for
  - True copy of student transcripts
  - Original replacement
- Needed for employment and immigration applications
  - Most applications are done online and remotely

# Why digitally sign student academic transcripts?

- Fraud
  - Fake transcripts can readily be purchased for your university
    - http://www.phonydiploma.com/Fake-Diploma-From-Australian-University.aspx
    - http://www.news.com.au/finance/work/the-great-aussie-degree-scam-forgers-raking-in-thousands-selling-bogus-qualifications/story-fnkgbb3b-1227284475119
  - When fake transcripts are accepted as legitimate, it is like stealing the intellectual property of the university, which students pay and work hard for
  - Allows fraudster to obtain/receive benefits under false pretences
    - legitimate students could miss out on employment positions
  - Could allow fraudsters into positions of trust, skill and professionalism which they are not qualified, causing harm to public people or property, eg doctors or engineers

# Why digitally sign student academic transcripts?

- Other methods are are less effective, unreliable and inconvenient
  - Requires prior knowledge of the various security features of printed transcripts
  - Can’t verify security features unless the original  transcript is examined in person
  - No further independent checking needs to occur
  - No requirement for JPs etc to view and sign certified true copies

- Convenience and consistent with online recruitment methods
  - Generally students send job applications via email or web
  - The authenticity of the transcript can be obtained immediately online

# Why digitally sign student academic transcripts?

- Increases the value of the student
  - A relying party obtains immediate assurance that the transcript is authentic and has not been modified since it was signed
- Increases the value of the transcript compared to other legitimate transcripts without a digital signature
  - Without a digital signature, a relying party is unable to assess whether the PDF transcript is authentic or was modified after it was issued
  - Conceivable that employers would prefer students from universities which provide digitally signed transcripts
- Increases the value of the university and its academic credentials
  - Students would prefer universities preferred by employers

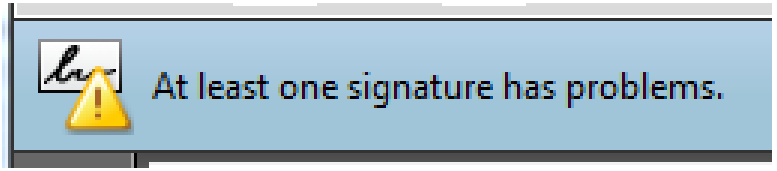
# Why digitally sign student academic transcripts?

- Builds trust and confidence in the teaching and learning services of universities that digitally sign their student transcripts
- Protects the intellectual property of the university
- Protects students from third party fraud
- Preferred by students and employers

# Demonstration

- PDF manual signing
  - Visible or embedded signatures
  - Single or multiple signatures
  - Examine the signature/certificate
- Valid and fully trusted signature

  - Issuing CA is in the Adobe Approved Trust List
  - Authenticity and integrity verified
  - Identity of signer is known and trusted, ie issued in accordance with the relevant CPS
  - Document has not been modified since it was signed
- Unknown identity
  - Issuing CA is not the Adobe Approved Trust List
  - Authenticity check fails
  - Not known if the identity is the person claimed
  - Document has not been modified since it was signed




- Untrusted signature
  - Issuing CA may or may not be on the AATL
  - Authenticity and integrity check fail
  - Document has been modified since it was signed


# Questions

k.kerr@auscert.org.au

cs@auscert.org.au