MANAGING RISK

PKI Interoperability by an Independent, Trusted Validation Authority

UNIK, Kjeller

Jon Ølnes, DNV Research & Innovation
12.06.2008

DNV – an independent foundation

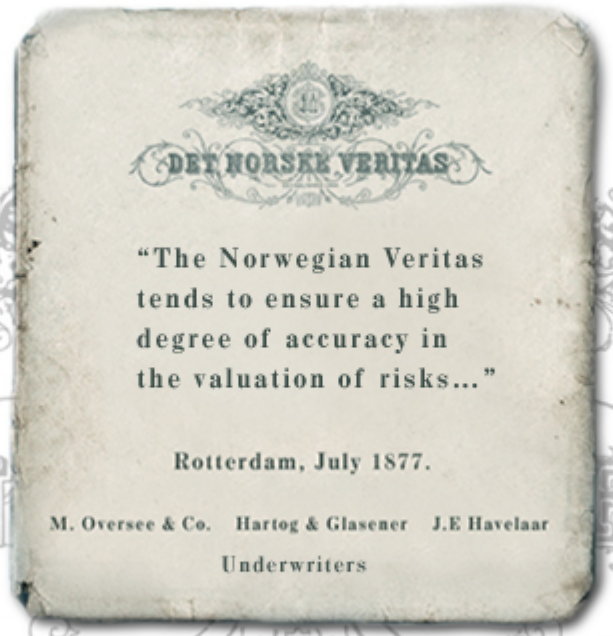
MANAGING RISK

- Purpose:
  - Safeguarding life, property, and the environment
- Vision:
  - Global impact for a safe and sustainable future

More than 140 years of managing risk

MANAGING RISK

- Det Norske Veritas (DNV) was established in 1864 in Norway
- The main scope of work was to identify, assess and manage risk – initially for maritime insurance companies



New risk reality

MANAGING RISK

- Companies today are operating in an increasingly more global, complex and demanding risk environment

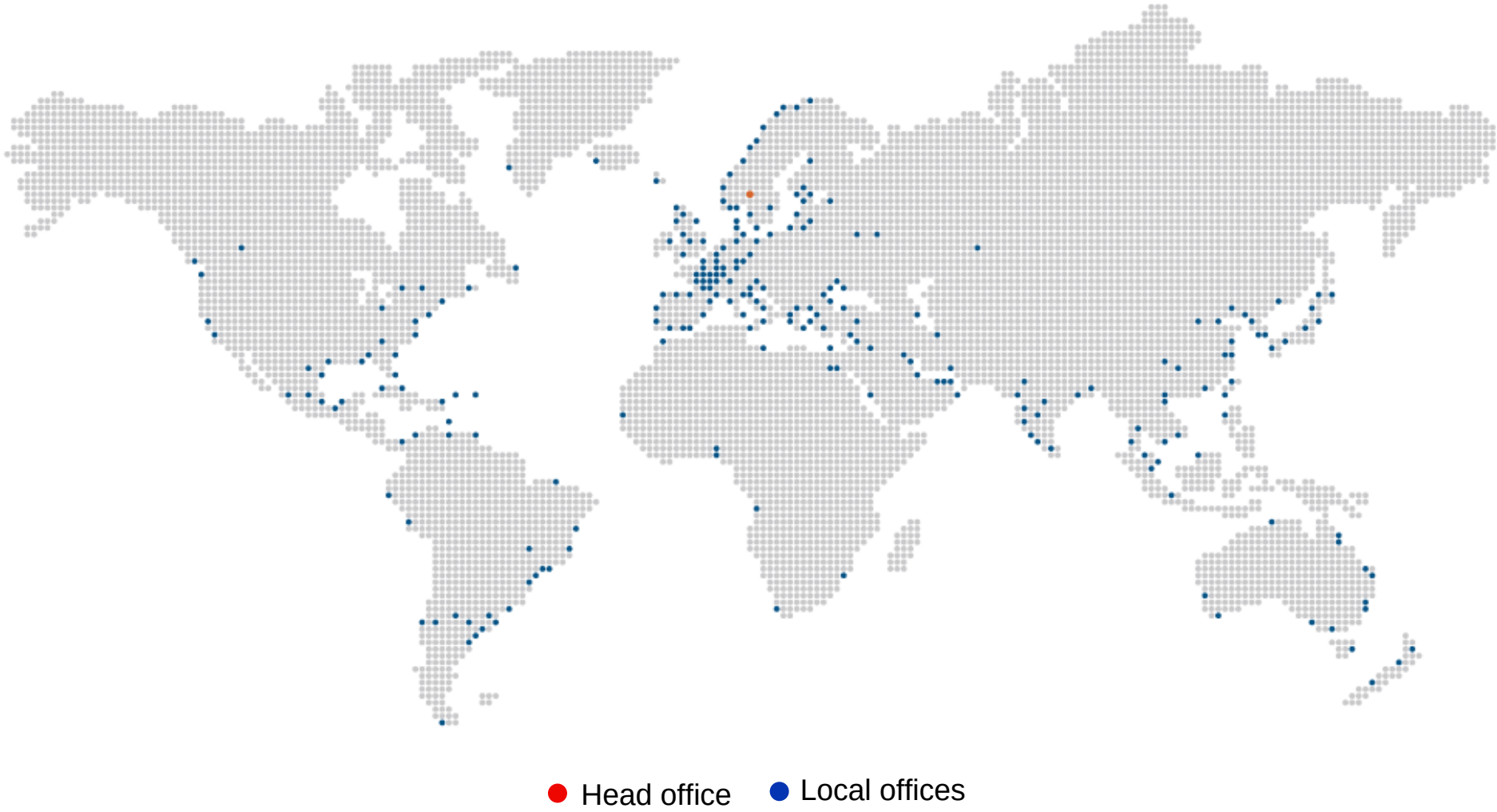
- Society at large is gradually adopting a “zero tolerance” for failure
- Increased demands for transparency and business sustainability
- Stricter regulatory requirements
- Increasing IT vulnerability

Core competence

MANAGING RISK

300 offices in 100 countries

MANAGING RISK

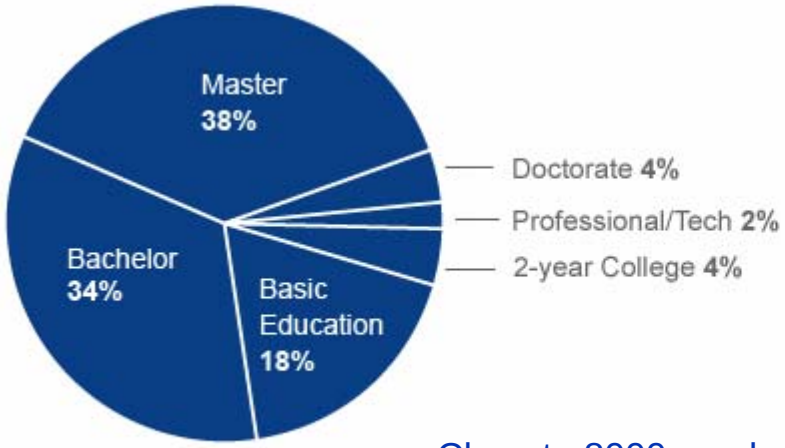


Our people – a vital resource

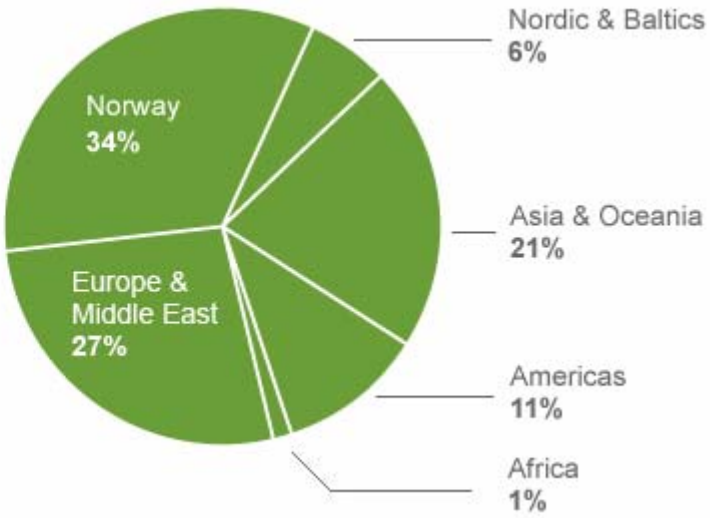
MANAGING RISK

- People are the core of DNV
- 85 nationalities

Competency chart



DNV staff around the world



Close to 8000 employees

Target industries

MANAGING RISK

Managing risk

Maritime

- **Ship classification**
- **Certification of materials and components**
- **Assessments and solutions**
- **Fuel testing**
- **Training**

Energy

- **Risk management consulting**
- **Qualification and verification**
- **Offshore classification**
- **Laboratory services**
- **Training**

Other prioritised industries

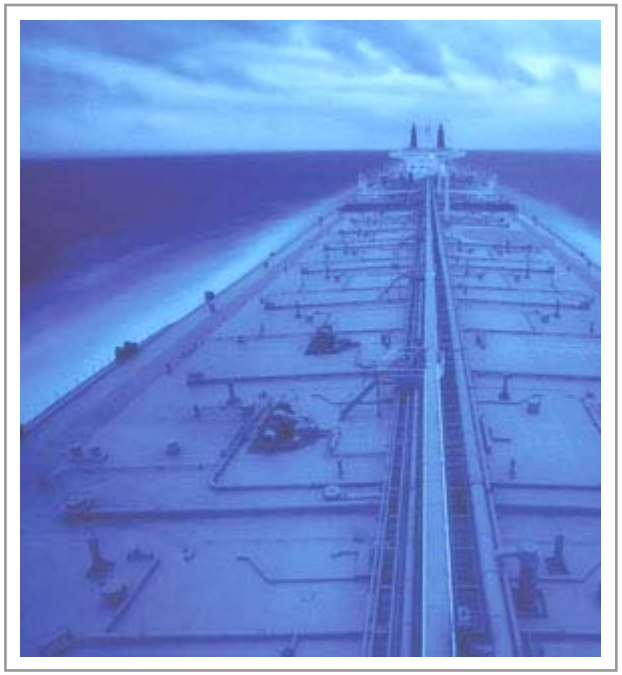
- **Automotive**
- **Defence**
- **Finance**
- **Food and Beverage**
- **Health care**
- **ICT and telecom**
- **Public sector**
- **Transportation**

Maritime

MANAGING RISK

DNV is a world leading classification society

- 16% of the world fleet to class
- 24% of ships ordered in 2006
- 70% of maritime fuel testing market
- Authorised by 130 national maritime authorities
- Continuous high performance in Port State Control worldwide

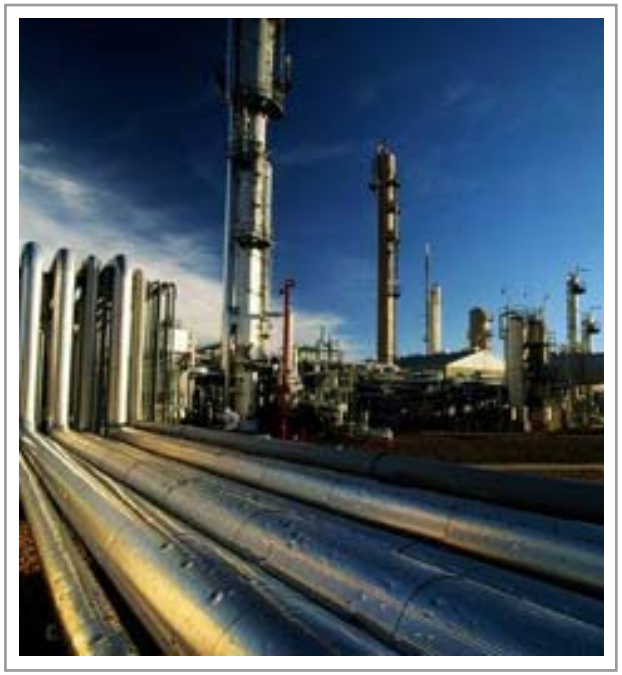


Energy

MANAGING RISK

Safeguarding and improving business performance

- Cross-disciplinary competence within risk, management, technology and operational expertise
- Our services and solutions are built on leading edge technology
- Offshore pipeline technology leader
  - DNV Offshore Rules for pipelines recognised as world class
- Deep water technology
  - Providing reliable verification and qualification of unproven technology
- Broad experience with LNG / Natural Gas



Services to industries

MANAGING RISK

- IT risk management services
- Business consulting services and solutions
  - Enterprise risk management
  - Safety, Health and Environmental (SHE) risk management
  - Change management
- Software products and services
- Training

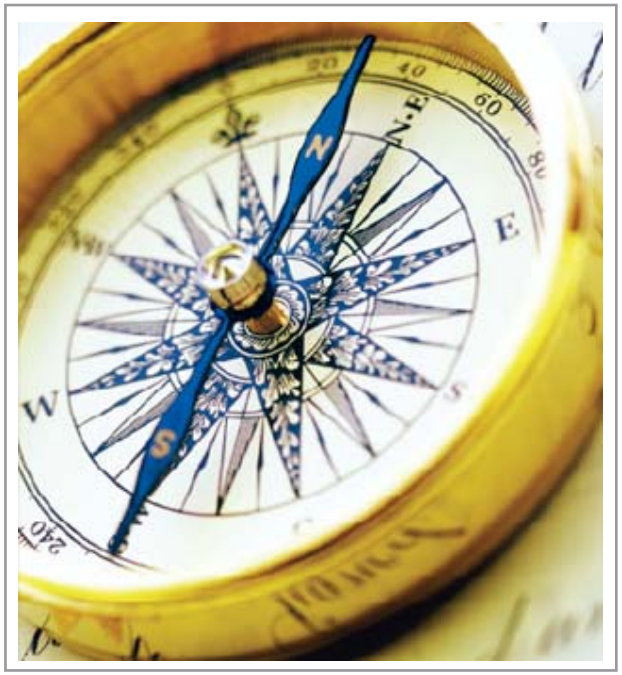
- Management system certification
- Climate Change
  - Voluntary emission reduction
  - CDM, JI, EU ETS
- Corporate Responsibility
  - Governance responsibility assessment
  - Supply chain management
  - Verification of sustainability reporting
- Product certification

Management systems certification services

MANAGING RISK

More than 80 national accreditations and 65 000 certificates issued worldwide

- Cross-industry certification
  - Quality – ISO 9001
  - Environment – ISO 14001
  - Occupational health and safety – OHSAS 18001
  - Information security – ISO/IEC 27001
- Industry specific certification standards
  - Automotive – ISO/TS 16949
  - Food safety – ISO 22000
- Risk Based Certification ™
  - A unique approach to management system certification



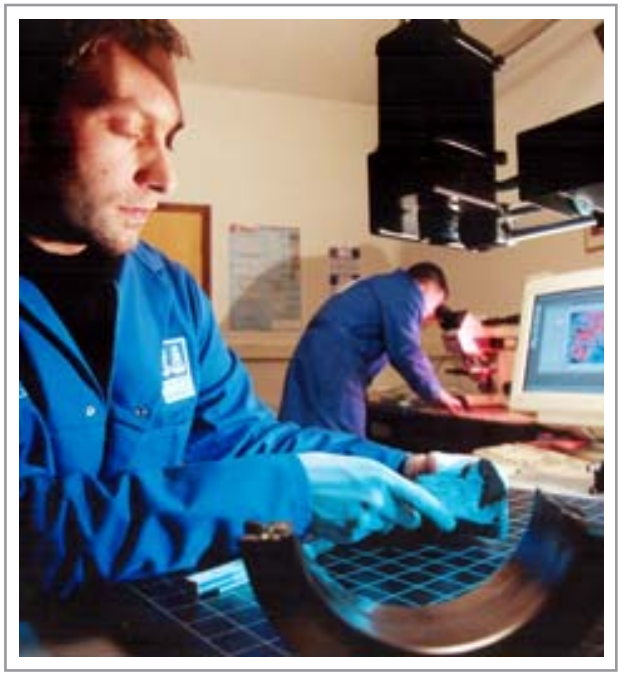
*Risk Based Certification is a trademark of Det Norske Veritas AS.

Research and innovation

MANAGING RISK

Competitive advantage from continuously updated knowledge and expertise

- DNV invests some 5% of revenue on Research and Innovation
- Enhance and develop services, rules, and industry standards
- Ensures DNV's position at the forefront of technological development
- Key research areas:
  - Maritime Transport Systems
  - Marine Structures
  - Future energy solutions
  - Information processes and technology
  - Biorisk
  - Multifunctional materials and surfaces
  - Arctic Operations



DNV and digital value chains

MANAGING RISK

- DNV has existed as an independent, trusted party for 140 years
  - Ship and process industry classification and certification
  - Certification to ISO 9000, ISO 14000, BS 7799 etc.
- Carry on this position to new areas
  - Digital value chains / processes between actors
  - Which trusted roles are needed for such processes?
  - Which roles may be of interest for DNV to take?
  - ”Safeguarding life, property, and the environment” applied on digital value chains
  - PKI and digital signatures are key elements in securing such processes

DNV's own PKI requirements (example)

MANAGING RISK

- Reshaping own business processes (e-processes)
- Strong need for signatures, e.g. issuing ship certificates
- Role as PKI Relying Party, e.g. receiving documentation from actors

➢Global PKI interoperability is required for these e-processes

➢Signed documents must be verified by other parties than those involved in the signing process

built in Finland to DNV Class

equipment from Germany

steel from South Korea

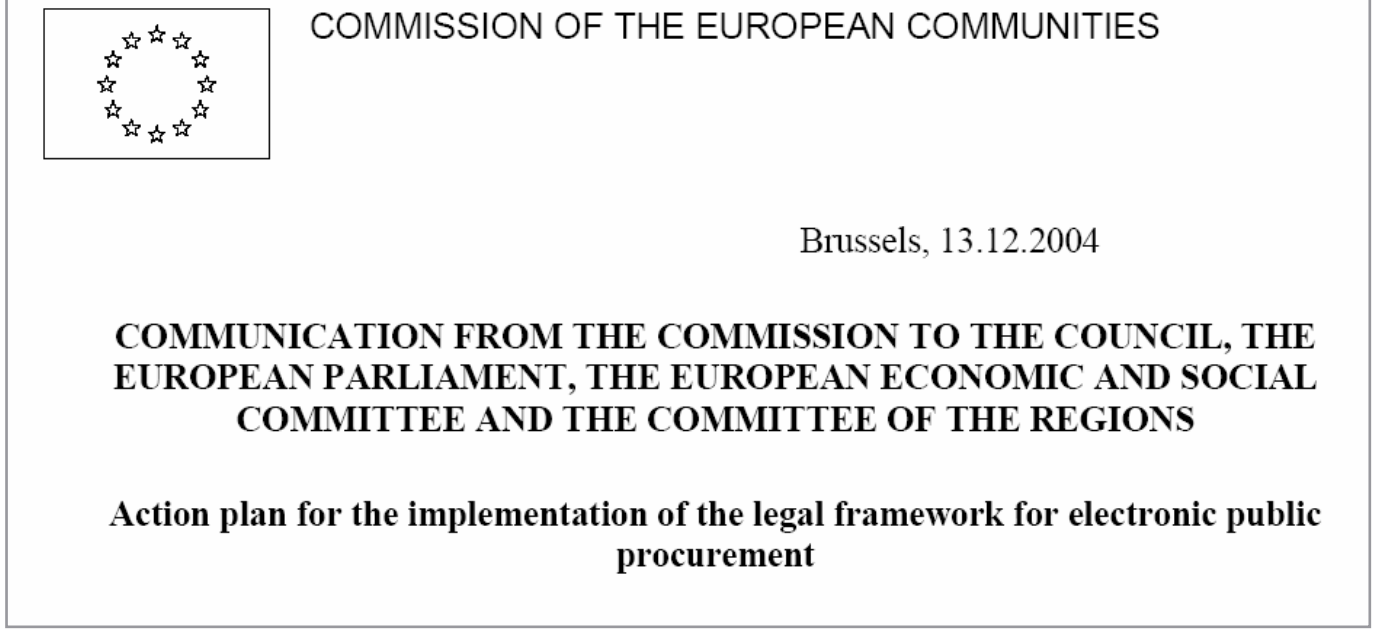
USA based ship owner

Bahamas registered

Insured in UK, calls port in Singapore, ….

Example: e-Procurement in EU public sector

MANAGING RISK



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 13.12.2004

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Action plan for the implementation of the legal framework for electronic public procurement

- *"Directives oblige any public purchaser in the EU to effectively recognize, receive and process tenders submitted, if required, with a qualified signature and their accompanying certificates,* ***regardless of their origin within the EU or their technical characteristics****"*
- *"The existing* ***significant differences between qualified signatures*** *…. should therefore be reason for great concern. The* ***interoperability problems*** *detected despite the existence of standards …. pose* ***a real and possibly persistent obstacle*** *to cross-border e-procurement."*

eSignatures, EU Directive

MANAGING RISK

- **Electronic** signature
  - In principle anything that binds an actor to an action or to data
  - In a way that can somehow be documented
- **Advanced** electronic signature (i.e. **digital** signature)
  - Under the sole control of the signer and uniquely linked to the signer
  - Linked to the data in such a way that subsequent changes are detected
  - Only available technology is PKI-based digital signature
- **Qualified** electronic signature
  - Advanced signature using a qualified eID and a certified signing device
  - In European countries granted by law the same effect as a handwritten signature if the transaction can be carried out digitally
- Notes:
  - A non-qualified signature shall not unduly be denied legal effect
  - **European** definitions referring to **European** standards

Why digital (advanced) eSignatures?

MANAGING RISK

- Compliance – where such signatures have to be used
- Improved business processes
  - Signing as explicit steps in processes
  - Internal and/or towards partners and external bodies
- New or improved services to customers
  - Better functionality integrated, e.g. finance/credit agreements
  - Easier to enrol new customers with acceptable eID
- Security
  - Part of improved quality of services or processes
  - Signatures should not be introduced for security reasons only
  - Main feature: Protects against the legitimate counterpart
    - Need depends on trust between the parties

Do we think too much in paper-terms?

MANAGING RISK

- On paper, signing implies consent
  - The direct parallel is (too) often drawn to claim that eSignature is necessary
- Electronically, consent may be expressed in many ways
  - Digital/advanced eSignature
  - Click “submit” during an authenticated session
    - Submitted data and logs constitute the trace
    - System (and logs) may be run by an external, trusted party
  - Requirements depend on mutual trust
- Only a person can sign by hand – signature binds to the person only
  - An eSignature binds to the name in the eID
    - Why does the signer have to be a person?
    - E.g. corporate signatures on e-invoices (person is not relevant)
    - What about automated transfer between systems (e.g. accounting system to tax report system) with no person involved?
- Effects the way we define the term “signature”
  - Cannot state in regulations: Signature required on paper but not electronic
  - But can define what “electronic signature” (consent) means in certain contexts

Legislation in general

MANAGING RISK

- Most industrialized countries have legislation in place
  - Digital communication allowed for most purposes
  - E-signatures recognized for most purposes
  - E-signatures required for certain purposes
- Contents of legislations differ
  - Some focus on advanced signatures (or even qualified in Europe)
  - Some allow “simple” eSignatures for many purposes
- Incompatibilities or inconveniences may exist
  - National accreditation schemes hamper cross-border traffic
  - Qualified signatures required in some countries – only available in about half the EU member states and not outside of Europe

Status of use: National approaches and islands

MANAGING RISK DNV

- Government services target a national audience
  - Only one or a few selected eID issuers accepted for a service
  - Even public procurement, which is by law deemed to be open across the EU (IDABC Preliminary Study on the Interoperability of eSignatures for eGovernment Applications)
- Same goes for most private services
  - E.g. banking and commercial services

- Islands: Sectorwise national or international interoperability schemes
  - SAFE: International initiative in pharmaceutical industry
  - TSCP: Defence and aerospace
  - IdenTrust: International banking, mainly inter-bank
  - Federal-Bridge: US government (similar in some other countries)
  - WebTrust: Certification of eID services
  - ChamberSign: European chambers of commerce
  - Educational: USA and Europe
  - Grid computing
  - OGTS: Oil and Gas Trust Scheme
  - … and more

The eID/eSignature interoperability challenge

MANAGING RISK

(Signature used below – same goes for any eID usage.)

1. eID holder: Use the same eID for signing towards any counterpart
2. Receiver (relying party): Validate and accept signatures and eIDs from all relevant counterparts, no matter the eID issuer of the counterpart
3. Other parties: Verification of signed documents may (later) be required by parties not involved in the signing process

- The challenge is on the receiver

The interoperability challenges

MANAGING RISK

1. Signing
   - Local signing always possible but web interface signing is not standardized
2. Signature *verification* (including eID validation)
   - Technicalities – complex but achievable
3. Signature (and eID) *acceptance*
   - The signature can be verified, does it also have sufficient quality?
   - Legal or other requirements that must also be met?
   - Risk management decision
4. What does the signer's name mean and which authorizations are represented?
   - Semantics of the name in eID – usually a person name, perhaps other attributes
     - Use of national or internal identifiers for persons and organizations
   - How is this linked to businesses, roles, and authorizations?
     - These are usually not represented in the eID
5. How are signatures used in the (business) processes?
   - What needs to be signed at what steps of the process, and what do signatures imply?
   - Part of specification of e-business processes

Infrastructures and trust

MANAGING RISK

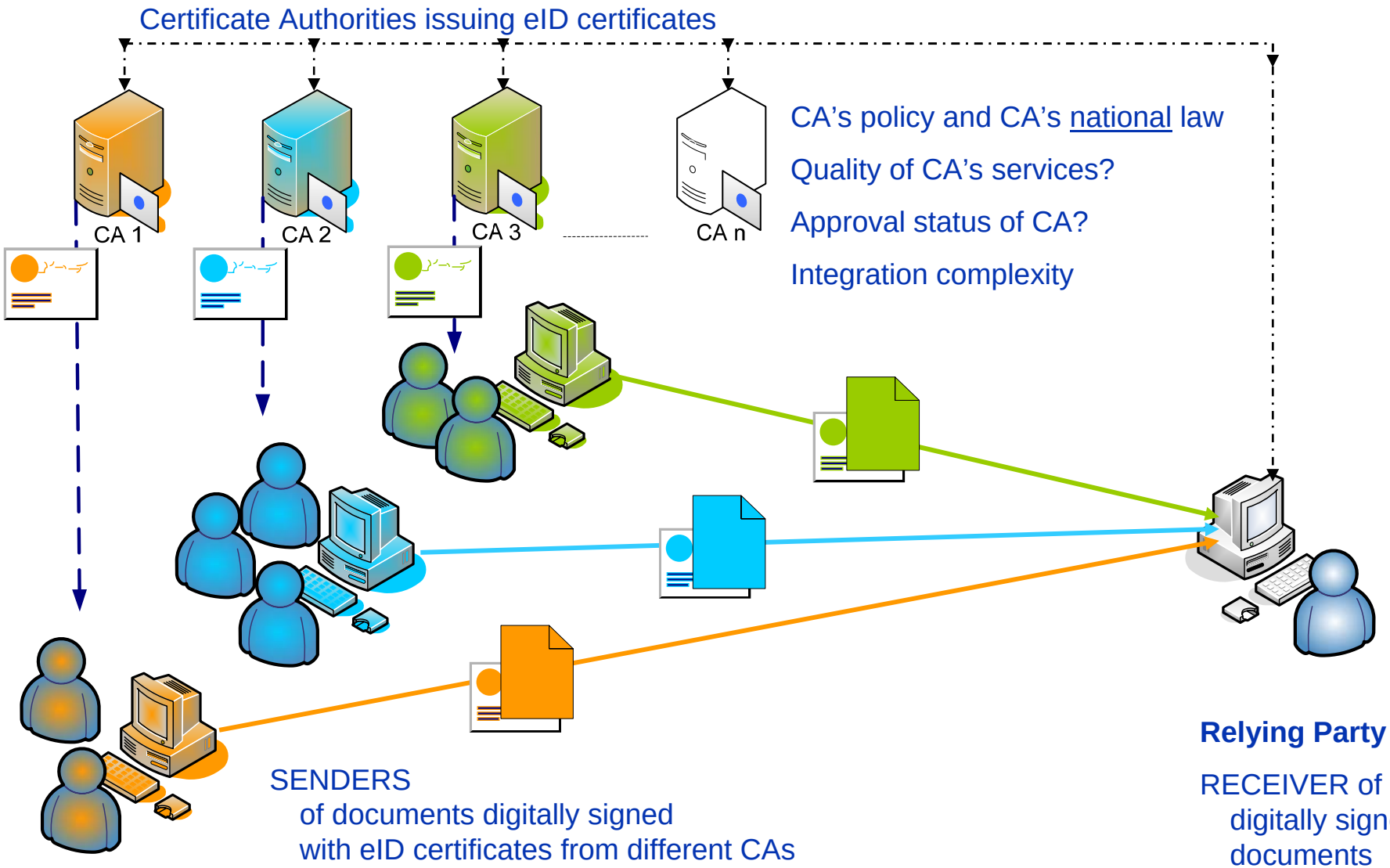
- The eID holder has one trusted party: The eID issuer
  - Certificate Authority (CA)
  - The PKI – Public Key Infrastructure
- The receiver (relying party) today has no such party
  - Validation Authority: One trusted party even for receiver
- Infrastructures are introduced for two reasons:
  - Scalability – numbers of users or actors
  - Trust – risk management, assessed quality, liability
- If either one hits, you may need a PKI and a Validation Authority

Risk management requires agreements

MANAGING RISK

- Relying on general statements in policies of eID issuers is too risky
  - Written in foreign language, referring to foreign legislation …
- A receiver cannot enter agreements with all eID issuers
  - Cannot by itself judge quality and liability
  - Unknown risk situation
- An eID issuer cannot have agreements with all possible receivers
  - Europe: In principle unlimited liability for issuers of qualified certificates
  - Can be regulated by agreements
  - Unknown risk situation for the CAs
  - One reason for the existence of “islands”

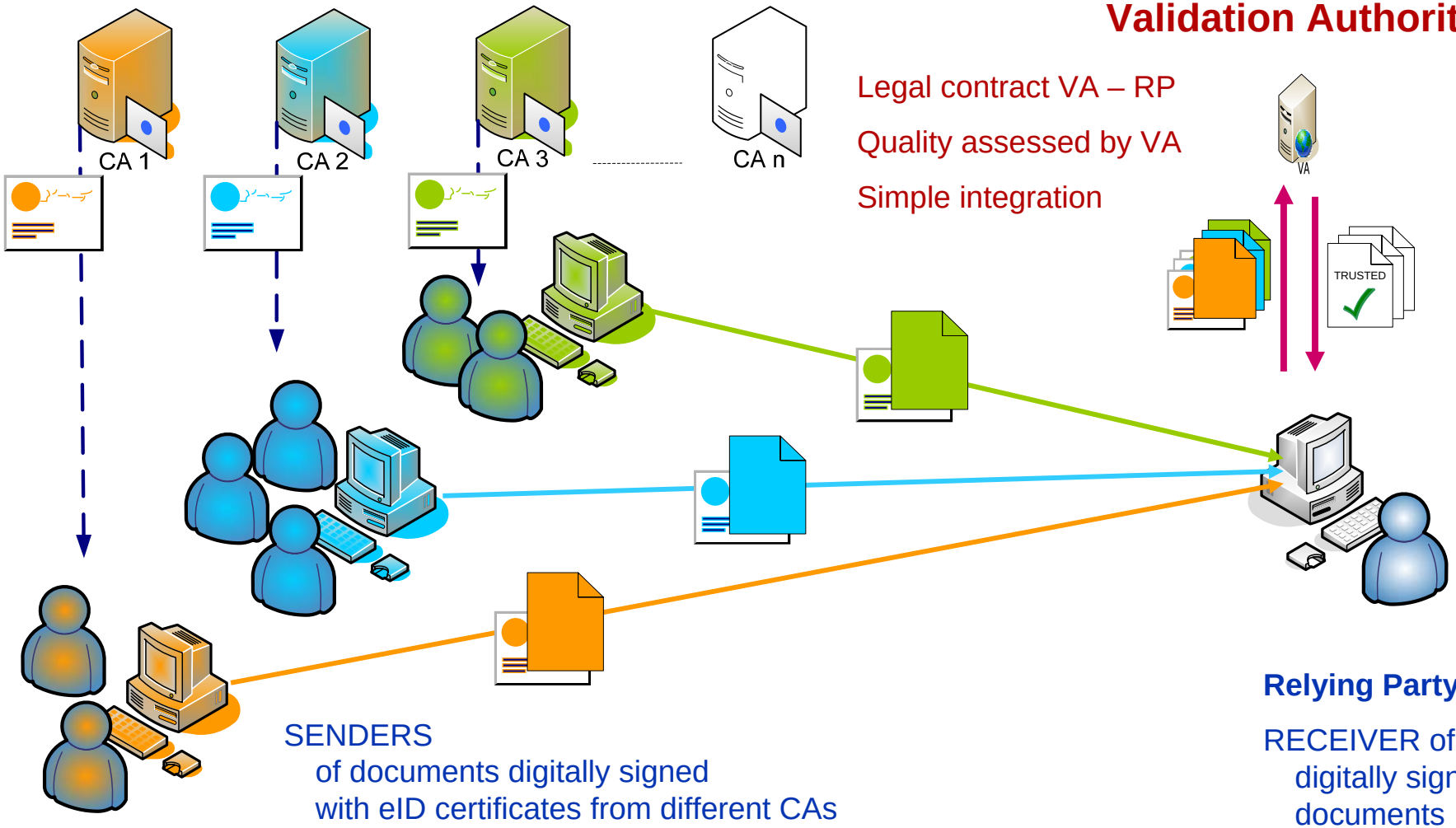
RP's situation without a Validation Authority



Role of a Validation Authority

MANAGING RISK

Certificate Authorities issuing eID certificates



Validation Authority

Legal contract VA – RP

Quality assessed by VA

Simple integration

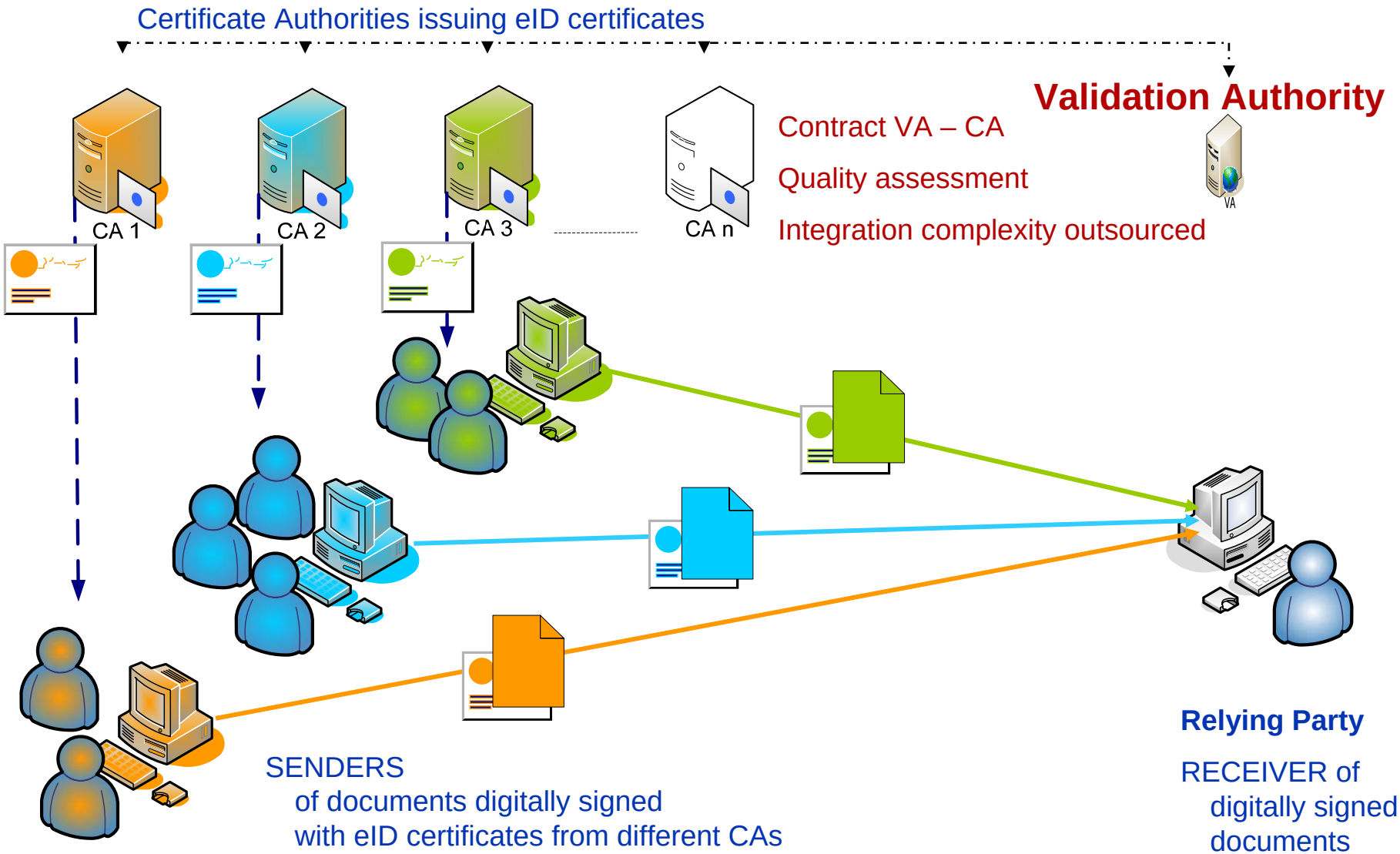
SENDERS
of documents digitally signed
with eID certificates from different CAs

Relying Party

RECEIVER of
digitally signed
documents

The back-end side of the Validation Authority

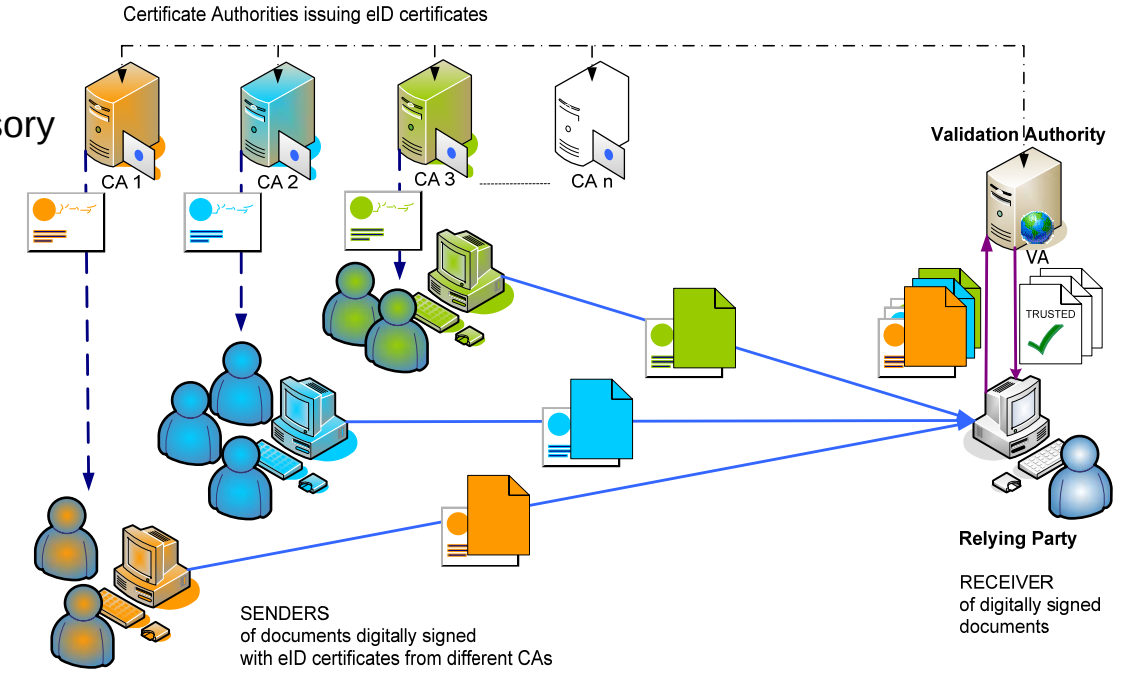
MANAGING RISK



Requirements to the Validation Authority

MANAGING RISK

- Trustworthiness
  - Accreditation/registration at Supervisory Authorities (as for CAs) ?
  - Brand
- Independence from CAs
- Responsibility and liability
  - At the VA, not individual CAs
- Contract with RP
  - **From national law to contract law**
- Ability to handle many CAs
- Quality of service
- Availability of service



"One-stop-shopping" for the receiver

“One stop shopping” for Relying Parties

MANAGING RISK

- The VA is an independent trust anchor, trust is not delegated from the CAs
  - Challenges the PKI axiom that only a CA may be a trust anchor
  - The VA handles each CA individually
  - Must be independent from any CA – treat all CAs on equal terms
  - Eliminates need for certificate path discovery and validation
- One agreement for processing of certificates, irrespective of origin
  - One point of contact and billing
- Proper management of risk and liability
  - Removal of complexity
  - Classification and assurance of quality
  - Acceptance of liability (agreement RP/VA)
  - Transfer of liability (agreements VA/CAs)
- One software integration
  - Web Service interface proposed for the VA service
- Scalability
  - Acceptance of new customers, with certificates from “new” CAs

The business case – win * 4

MANAGING RISK

1. The Relying Party
   - One stop shopping and proper risk management
2. The Certificate Holder
   - Possibly better reuse of the certificate
3. The Certificate Authority
   - Better reuse of certificates – more relying parties
   - Agreements with RPs through VA – improved risk management
   - The VA is not visible and shall not jeopardise CAs' business models
   - CAs tend to react positively to the idea of a VA …
4. The Validation Authority
   - On-line services that customers are willing to pay for(?)

- There should be a competitive market for VA services
  - Open specifications, in the end preferably standardised

eID quality and approval status

MANAGING RISK

DNV's current scheme, proposed as suitable for Europe:

0. Inadequate or non-determined level: Very low confidence or assessment not possible.
1. Low level: Low confidence in eID.
2. Medium non-approved level: Medium confidence eID with no formal registration/approval status
3. High non-approved level: eID quality is at or very close to qualified level, but eID issuer is not registered/approved by assigned inspectorate/authority. (Note that qualified eIDs can only be issued to persons, not other entities.)
4. Non-qualified approved level: eID is not marked as qualified; eID issuer is registered/ approved according to a (national) scheme for issuers of non-qualified eIDs.
5. Qualified approved level: Qualified eID registered/approved according to applicable law to the issuer. Qualified signatures not supported (no certified signing environment).
6. Qualified signature level: eID is marked and registered as for level 5, and use of a certified signing environment is mandatory. This level supports qualified signatures according to the EU Directive on electronic signatures.

Signature quality

MANAGING RISK

- Calculation formula:
  Signature quality = eID quality + hash algorithm quality + public key algorithm and key length quality
  - If any quality parameter is 0, signature quality is 0 regardless of the values of the other two quality parameters. The signature is considered too weak to be trusted.
  - If eID quality is 6, and both other quality parameters have value 2 or higher, the signature quality is 20. This value thus indicates a qualified signature according to the EU Directive.
- Quality values for cryptographic algorithms with key sizes:
  - Quality 0: Inadequate - should not be trusted.
  - Quality 1: Marginal - reasonably secure for short term
  - Quality 2: Trustworthy for approximately five years.
  - Quality 3-6: Increasing levels of quality
  - (Adapted from NIST recommendations to US Government, aligned with similar recommendations in Europe)

Classification (ongoing development)

MANAGING RISK

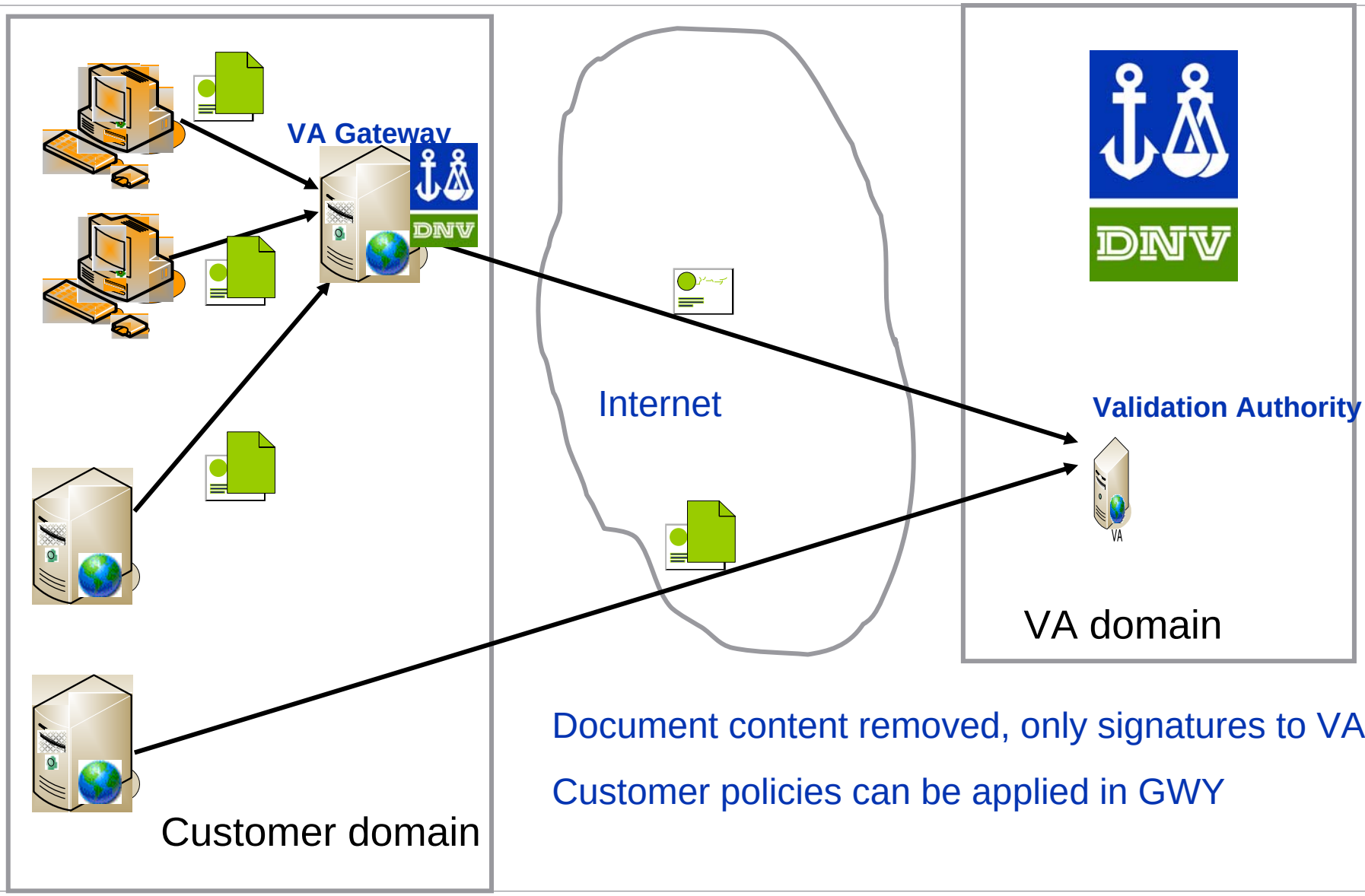
- Objective, globally applicable criteria for eID classification
  - Base on existing work (Federal Bridge CA (USA), EU qualified level, ETSI Normalised Certificate Policy, American Bar Association (ABA), Web Trust, T-scheme, Asia PKI Interoperability Guide, Extended Validation SSL certificates etc.)
  - Acknowledge national accreditation schemes
- Determine a eID issuer's class from policy and other documentation
  - Plus perhaps other information on eID issuer and owners (customer base, credit rating, income versus expenses etc.)
  - Classification may be less stringent than policy mapping for cross-certification
- Assess assurance level for classification
  - Study of documents, self-assessment, surveillance, third party audit report, certifications etc.
- Publish quality classification
  - Numerical value (0-N)
  - Profile (structure) of values for different quality parameters
- **Criteria should be turned into standards**
  - **And be used as basis for third party certification of eID issuers**

Validation policies

MANAGING RISK

- VA performs quality rating of eID issuers
  - Quality as stated in policy (profile created, numerical value may be derived)
  - Legal standing
  - Compliance
  - Liabilities
  - Financial standing and market position
- VA customer (receiver of eSignatures/eIDs) amends this policy
  - Quality requirements (numerical value or profile)
  - eID issuers that are explicitly trusted or not trusted
  - Criteria such as nationality
- The eID issuers' policies should be obeyed
  - Certain receivers (e.g. due to nationality) may be prohibited
  - Certain use cases may be prohibited

The VA Gateway



Document content removed, only signatures to VA

Customer policies can be applied in GWY

VA status

MANAGING RISK

- DNV VA services just recently launched as commercial service
  - http://va.dnv.com
  - The Norwegian Electronic Public Procurement Portal
  - Pilot with StatoilHydro later this year
  - PEPPOL (Pan-European Public Procurement On-Line)
    - EU-wide pilot that will target eSignature interoperability
- CertiVeR, Spain
  - http://www.certiver.com/
- Spanish national solution
- Lots of activities – technical integration of many CAs in one validation interface
- IDABC Preliminary Study on Mutual Recognition of eSignatures for eGovernment Services proposes network of co-operating VAs in Europe
  - Protocols etc. must be standardized
  - What are requirements for a national instantiation of a VA?
    - Given that contract law and not national law is applied
  - What are the requirements for governmental control over VAs?
    - Given contracts with VA operators
- Think globally, start with Europe

What about trust structures?

MANAGING RISK

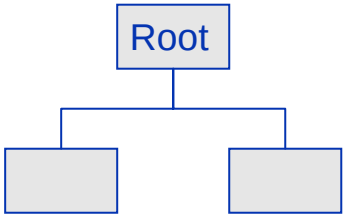
- Start with your own CA to obtain a trusted copy of remote CA's public key
- May indicate quality (policy mapping, hierarchy base policies)

- Revocation checking must still be done towards remote CA
  - May be a software integration and efficiency problem
- Liability still resides with remote CA
  - Check the CA's policy
- Path processing (especially discovery) can be very complex

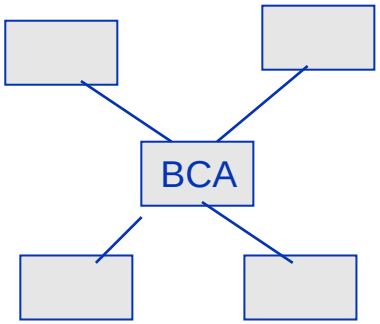
Trust Models

MANAGING RISK

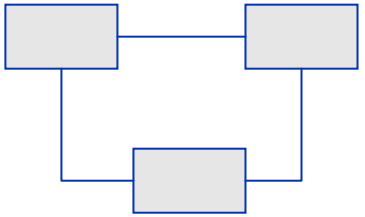
Hierarchy



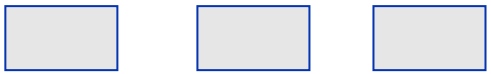
Bridge CA



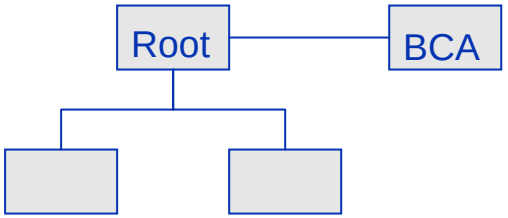
Mutual cross-certification



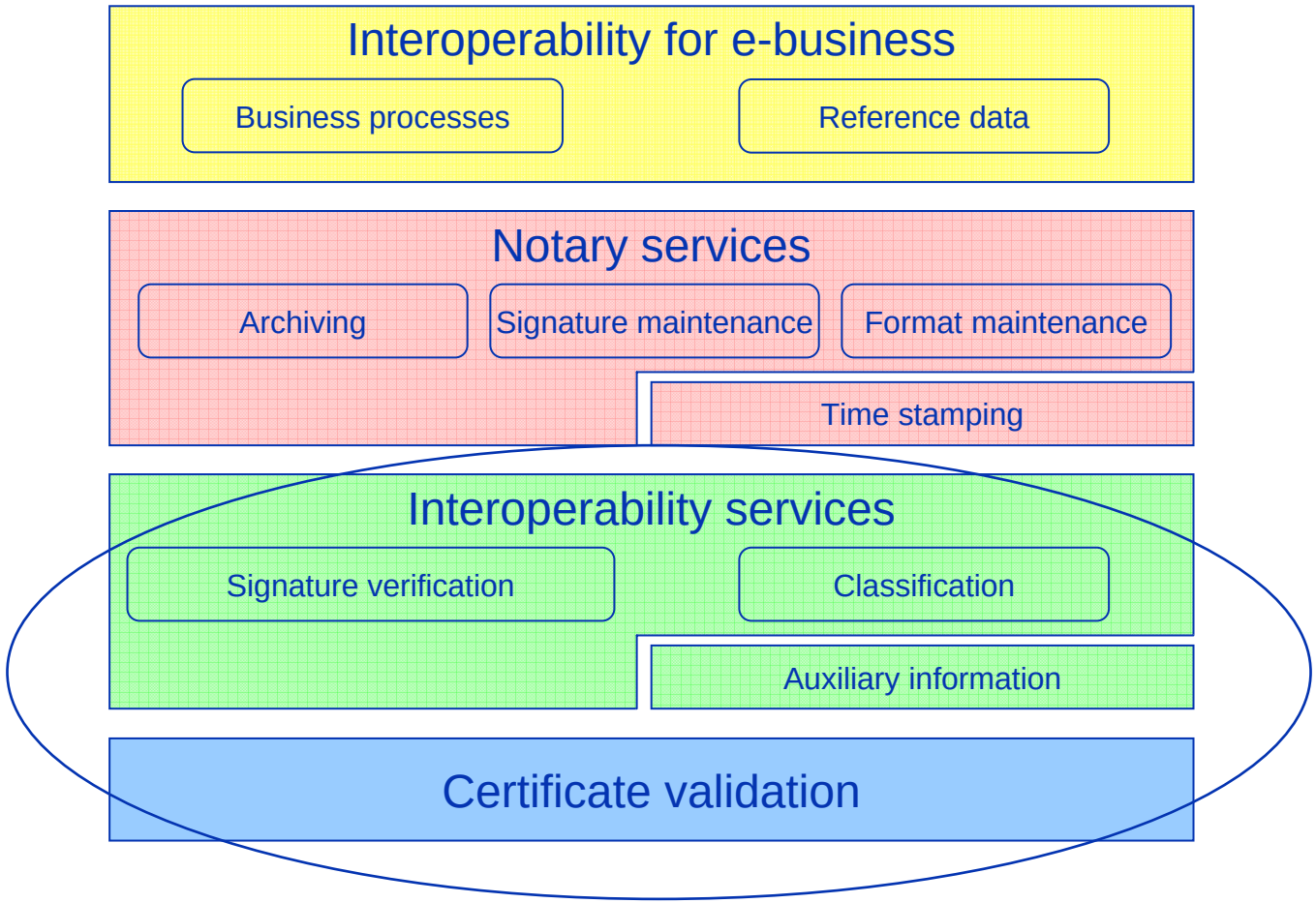
Trust list



Hybrid

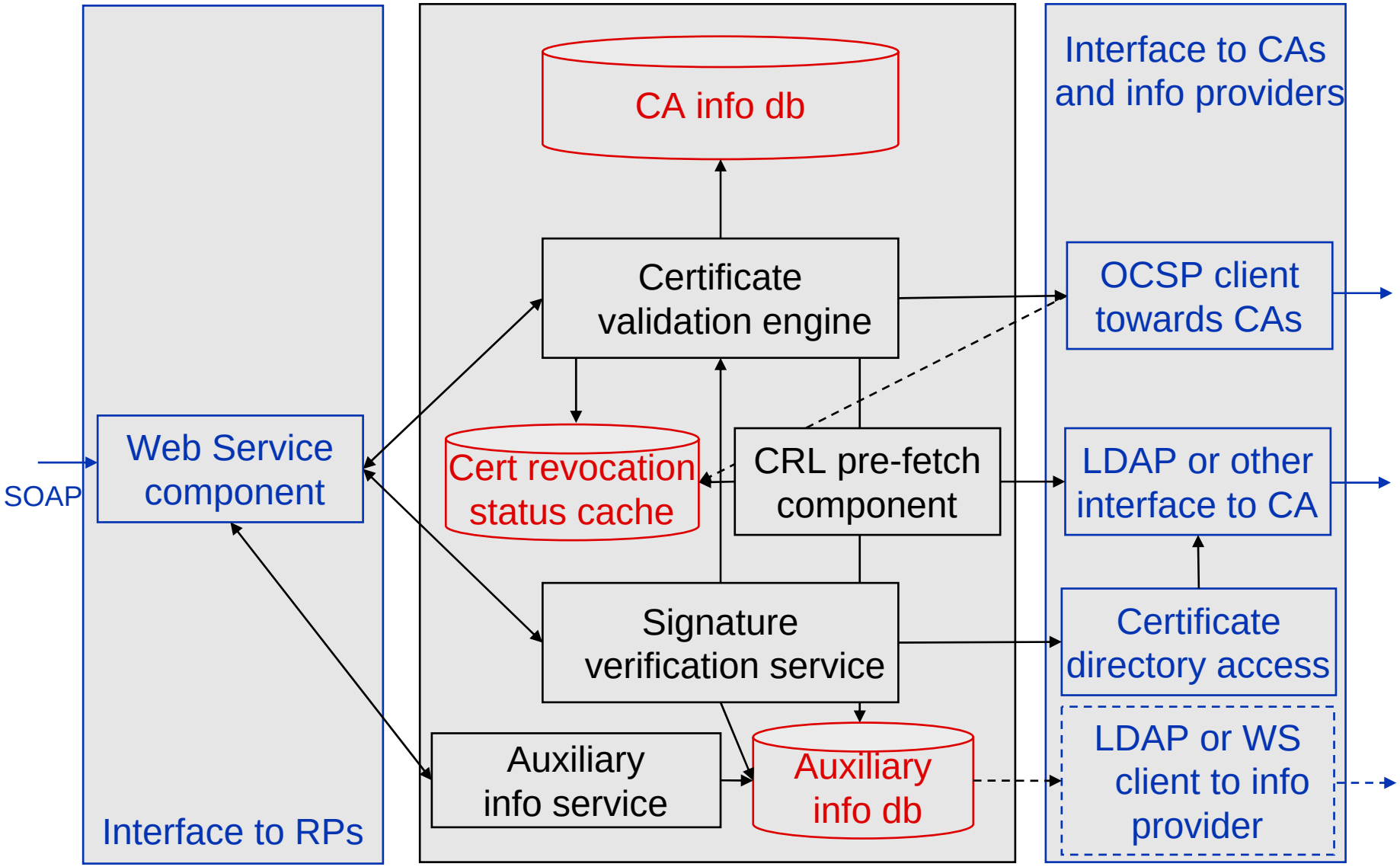


VA services


Interoperability for e-business
Business processes
Reference data
Notary services
Archiving
Signature maintenance
Format maintenance
Time stamping
Interoperability services
Signature verification
Classification
Auxiliary information
Certificate validation

VA services architecture

MANAGING RISK



Some implementation issues

MANAGING RISK DNV

- Interface/integration towards relying parties
  - Web Services / SOAP preferred
  - Based on the XKISS part of XKMS
  - Security and authentication by SSL, and/or XML-DSIG and XML-Encryption
- Interface towards CAs (and other information providers)
  - CRL pre-fetch to VA preferred – polling, not only on schedules
  - OCSP client towards CA must be supported
  - LDAP or other to fetch certificates when only reference given
- Information stored locally
  - Enables historical validation, according to time-stamp parameter in request or time-stamp in old, signed document
  - For audit purposes and to prove reason for answers
- DNV's development partner is Ascertia Ltd. (UK and Pakistan)
  - http://www.ascertia.com

ascertia

Signature verification Web Service

MANAGING RISK

- Request (may be signed) contains:
  - One digitally signed document or pair(s) of signature(s) and hash value(s) belonging to the same document
  - Optionally quality requirements to signatures and eIDs (default values may be configured in the VA for the specific relying party)
  - Optionally flags for requested “respond with” parameters
- Response (always signed by the VA) contains:
  - Overall assertion (trusted, not trusted, indeterminate) for document
  - Assertions for each signature and eID (valid, invalid, indeterminate, insufficient quality)
  - Names (DN) from all certificates
  - Values for “respond with” parameters
- Other requirements
  - Should handle all signature formats (PKCS#1, PKCS#7, CMS, PDF, XML DSIG, ETSI TS 101 733, ETSI TS 101 903 and possibly more)
  - Should handle all cases of nested and independent signatures
  - Must handle all necessary hash and crypto algorithms

eID certificate validation Web Service

MANAGING RISK

- Request contains:
  - eID certificate(s) (support for certificate chains to be added)
  - Optionally quality requirements to certificates (default values may be configured in the VA for the specific RP)
  - Optionally flags for requested “respond with” parameters
- Response contains:
  - Assertions (valid, invalid, indeterminate, insufficient quality) for all eIDs
  - Name (DN) of eID holder(s)
  - Values for “respond with” parameters
- Other requirements
  - Validation based on direct trust in the CA – no need for certificate chains
  - Must handle all necessary hash and crypto algorithms

Respond with parameters (extensible)

MANAGING RISK

- Key value (the public key)
- Hash algorithm
- X.509 certificate chain
- X.509 CRL
- Subject key identifier
- OCSP (from CA)
- Time stamp
- Signed hash (decrypted hash)
- Content (signatures removed)
- Signature quality level
- Certificate quality level
- Key usage (from certificate)
- Extended key usage (from certificate)
- Basic constraints (from certificate)
- Valid from (from certificate)
- Valid to (from certificate)
- Certificate serial number
- Issuer name (DN of CA)
- CRL URL
- CRL number

Prerequisites and challenges

MANAGING RISK

- PKIs must be sufficiently ”open”
  - Some PKIs require each relying party to install particular software
  - The CAs’ business models must support a VA service
- Privacy
  - Do not track use of certificates across RPs!
  - Sufficient security of logs and other information
- VA services and relying party preferences
  - A VA service may be ”one size fits all” (base validation policy issued by VA)
  - Or configured to the needs of the individual VA customer
    - E.g. specify particular rules for CAs that shall/shall not be trusted
    - Customer specific validation policies
- Availability of the VA (single point of failure)
  - Distributed architecture needed
  - Replication for performance and availability
  - Localisation “close” to customers may be required
- Legal challenges in some countries?

CRL archive, historical validation

MANAGING RISK

- The VA downloads CRLs from CAs to local archive
- Cache of revocation status and time of revocations
- Time parameter in request – ask for “historical validation”
  - Response states validity at the time requested
  - May also use time-stamps in signatures or signed document
  - Not possible for CAs that use OCSP only
  - Earliest time is start of caching for this CA
- Complements long-term signed data objects
- An interface not offered on-line by CAs today

Distribution architecture

MANAGING RISK

- A “hub of the world VA” will not scale
- Simplest distribution architecture: replication
- More advanced architectures will be developed
  - Distribution of:
    - VA service instances
    - CRL download services
  - Probably 1-2 central CRL archive sites
  - A VA service instance answers by itself (except possibly historical validation)
    - Efficient information distribution to all VA instances
    - Alternative is rerouting of requests to the appropriate VA

Miscellaneous

MANAGING RISK DNV

- Relationship to bridge-CAs and similar?
  - Co-exist – may even be mutual benefits
- What about CardSpace etc.?
  - Fits well – the relying party has to validate credentials even in this case
- What about protocols?
  - OCSP is too limited in functionality
  - SCVP: Why use a specialized protocol when standard Web Services does it all?
  - XKMS: We used this as a basis
  - OASIS DSS: Yes, we need to look closer at this
- Standardization?
  - We publish our specifications
  - Some of our work should in fact be taken over by standards bodies
- What is the attitude of the CAs?
  - CAs are positive! Better re-use of eIDs, risk management, CRL archive …
  - Plus income sharing based on proportion of the VA's traffic
- Number of CAs?
  - Estimated in the order of 100 public CAs in Europe (number of agreements needed)
  - Several 100s world-wide
  - Consolidation rather that proliferation expected
  - Some corporate CAs will need to be included
- What does it cost?
  - No definite answer. What's the value of a signature on a contract? Scanning cost of invoice?

Summary

MANAGING RISK

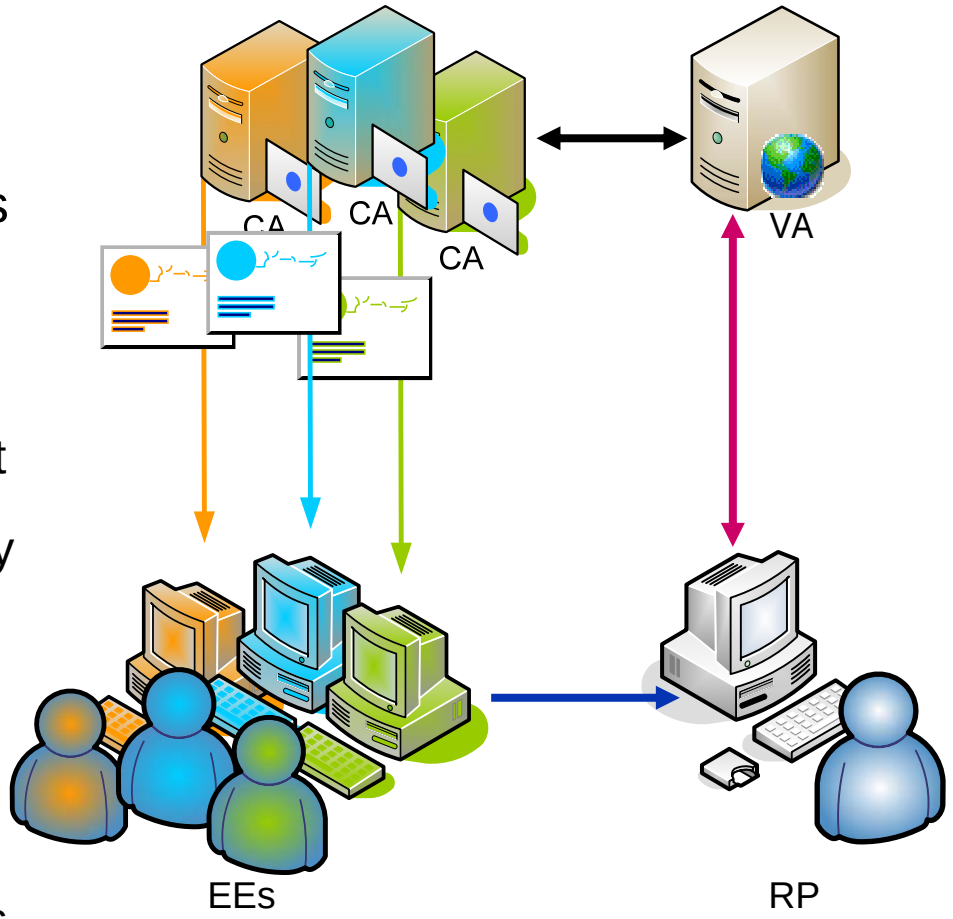
The Validation Authority:

An infrastructure providing a single trust anchor for the receiver of eIDs and eSignatures

- Handling complexity
- Providing risk and liability management
- Providing interoperability and scalability

➢Trust services to enable effective use of eID and eSignatures, realising the potential of PKI

- DNV VA is available to (pilot) customers
  - Development partner: Ascertia (UK)
  - http://va.dnv.com



ascertia http://www.ascertia.com

www.dnv.com

Thank you for your attention!

Jon.Olnes@dnv.com

+47 47846094