

# What's Wrong with the **Bylaws**

Ryan Sleevi / [sleevi@google.com](mailto:sleevi@google.com)



# What's Wrong with the ~~Bylaws~~ Auditors

Ryan Sleevi / [sleevi@google.com](mailto:sleevi@google.com)



# What's Wrong with the ~~Bylaws~~ ~~Auditors~~ Browsers

Ryan Sleevi / [sleevi@google.com](mailto:sleevi@google.com)



# What's Wrong with the ~~Bylaws~~ ~~Auditors~~ ~~Browsers~~ Ecosystem

Ryan Sleevi / [sleevi@google.com](mailto:sleevi@google.com)



Agenda

# Agenda

- Background
- Motivation
- History
- Current Issues
- Potential Solutions

Alternatively, you can think of it as:

- What's the problem?
- Why should I care?
- How did this happen?
- How bad is it?
- What can/should we do?

Agenda

## Agenda

- **Background**
- Motivation
- History
- Current Issues
- Potential Solutions

# A Problem of Terminology

# “Performance Audit”

CA/Browser Forum Bylaws, v2.1, § 2.1 (b)(6)



# “Point in Time Readiness Assessment”

Baseline Requirements, v1.6.0, § 8.1 ¶3

# “Period of Time Audit”

Mozilla Root Store Policy, v2.6.1, § 3.1.4

# “Key ceremony report”

Baseline Requirements, v1.6.0, § 6.1.1.1 ¶1

# “currently valid Audit Report”

Baseline Requirements, v1.6.0, § 8.1

# “Qualified Audit”

Mozilla Root Store Policy, v2.6.1 § 3.1.3

Microsoft Trusted Root Program

Requirements, r42, § 3, Item 1

# “Full Surveillance”

Mozilla Root Store Policy, v2.6.1 § 3.1.3

# “Publicly-Trusted Certificate”

Baseline Requirements, v1.6.0

# “Fail to pass [an] audit”

CA/Browser Forum Bylaws, v2.1, § 2.2 (b)(2)



# A Problem of Expectations

“How do I know  
this report is  
legitimate?”

“What reports are  
needed?”

“Is this report  
good?”

# A Problem of Results

# “EV keys <2048 bits that expire after 2010”

2009-10-04, Robin Alden,  
[management@cabforum.org](mailto:management@cabforum.org)

<https://cabforum.org/mailman/private/management/2009-October/002370.html>

# “Is the SSLiverse a Safe Place?”

2010, CCC 27, Peter Eckersley, Jesse Burns,  
Chris Palmer

<https://www.eff.org/files/ccc2010.pdf>

# AWS Labs Certlint

2016-01-16, Amazon

<https://github.com/aws-labs/certlint>



Agenda

## Agenda

- Background
- **Motivation**
- History
- Current Issues
- Potential Solutions

# What's the point of this talk?

- It's been **7** years since the Baseline Requirements
- It's been **13** years since the first CA/Browser Forum Meeting
- It's been **14** years since the first public review of audits (Mozilla)
- It's been **18** years since WebTrust for CAs 1.0
- It's been **18** years since ETSI TS 101 456 v1.1.1

- Baseline Requirements: Adopted 22 Nov. 2011 (Source: <https://cabforum.org/baseline-requirements-documents/> )
- First CA/Browser Forum Meeting: 17 May 2005 (Source: CA/Browser Forum Member Wiki F2F Meeting Calendar)
- First public review of audits as part of Root Store Policy: 30 March 2004 (Source: <https://wiki.mozilla.org/CA:CertificatePolicyV0.4> )
  - Microsoft had been requiring audits since 2001 (Source: [ftp://ftp.cert.dfn.de/pub/pca/docs/misc/MS\\_Root\\_Certificate\\_programV1.doc](ftp://ftp.cert.dfn.de/pub/pca/docs/misc/MS_Root_Certificate_programV1.doc) and <https://web.archive.org/web/20020402052029/http://www.microsoft.com/TechNet/security/news/rootcert.asp> )
  - Mozilla was distinct in first having public review of CA's CP, CPSes, and audits - which required understanding those documents to do the review
- WebTrust for CAs 1.0: Released 25 August 2000 (Source: <http://www.webtrust.org/homepage-documents/item65306.pdf> )
- ETSI TS 101 456: Released December 2000 (Source: [https://www.etsi.org/deliver/etsi\\_ts/101400\\_101499/101456/01.01.01\\_60/ts\\_101456v010101p.pdf](https://www.etsi.org/deliver/etsi_ts/101400_101499/101456/01.01.01_60/ts_101456v010101p.pdf) )

## What's the point of this talk?

- Make sure we have a common understanding of the history
- ... so that we can have a common vocabulary and understanding
- ... so that we can better explain our collective goals
- ... and can productively discuss what we're missing
- ... and how we can try to get there

# Why CAs Should Care

In the ideal world:

- Audits should streamline the inclusion process.
- Audits should reduce the risk of removal from trust stores.
- Audits should provide safe opportunities to gather feedback and improve; to mitigate rather than remediate.

## Why Auditors Should Care

- Audits need to provide value to the intended users: Browsers and Relying Parties (end users).
- There is a crisis of faith in the CA ecosystem in light of rampant **detectable** misissuance.
- There are opportunities to learn and adapt from the other schemes.

# Why Browsers Should Care

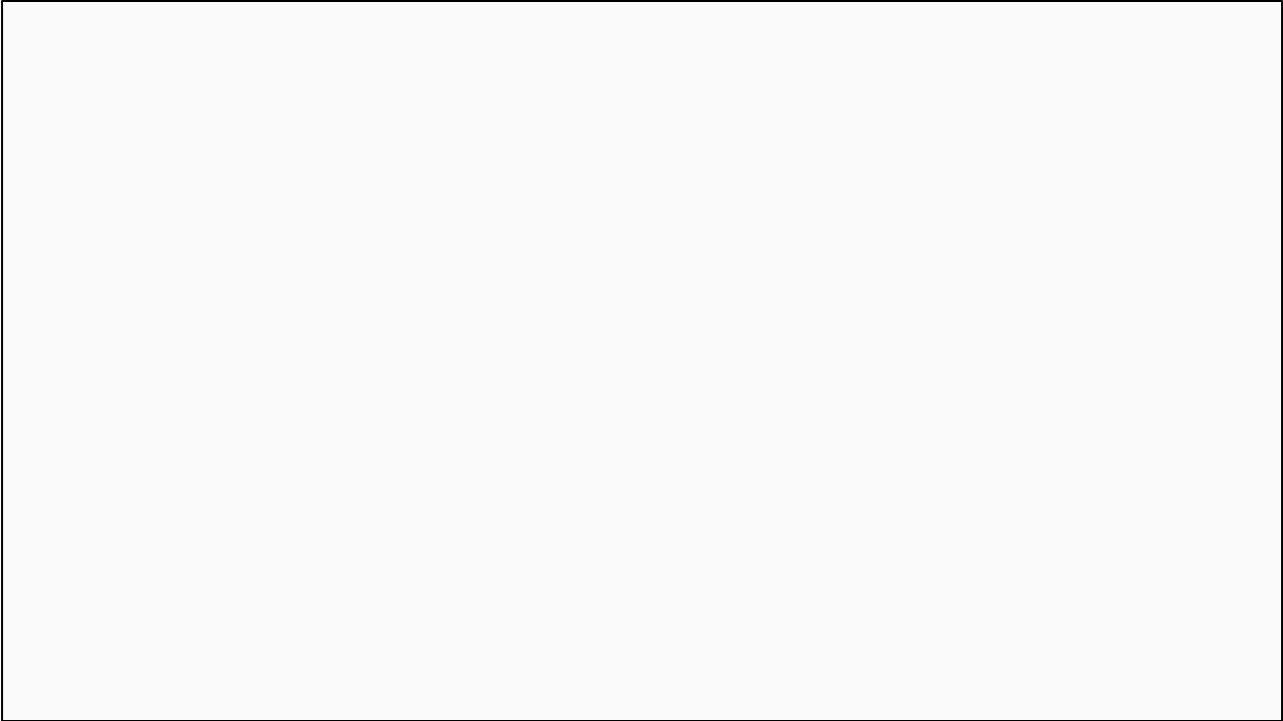
In an ideal world:

- Audits should reduce work, not increase it.
- Audits should be consistent quality and provide consistent results, regardless of the auditor or scheme.
- Audits should constantly be improving in rigor, thoroughness, and usefulness.

Agenda

## Agenda

- Background
- Motivation
- **History**
- Current Issues
- Potential Solutions

- 
- In the beginning, a whole bunch of standards groups created perpetual job security for the rest of us. Now the audit criteria were formless and empty, chaos was over the surface of the Web PKI, and the lawyers were hovering over the certificates. And the American Banking Association said “Let there be work”... and oh how there ever has been.
  - Slightly blasphemous joking aside, we need to pick a point to start - how far down the stack of turtles should we go before we pick a starting point to built the rest of the world on top of? Since this is about audits, I thought I’d start with the best direct ancestor for our collective family tree, and that’s the X9.79 PKI Practices and Policy Framework.



**X9.79 - PKI  
Practices and  
Policy  
Framework**

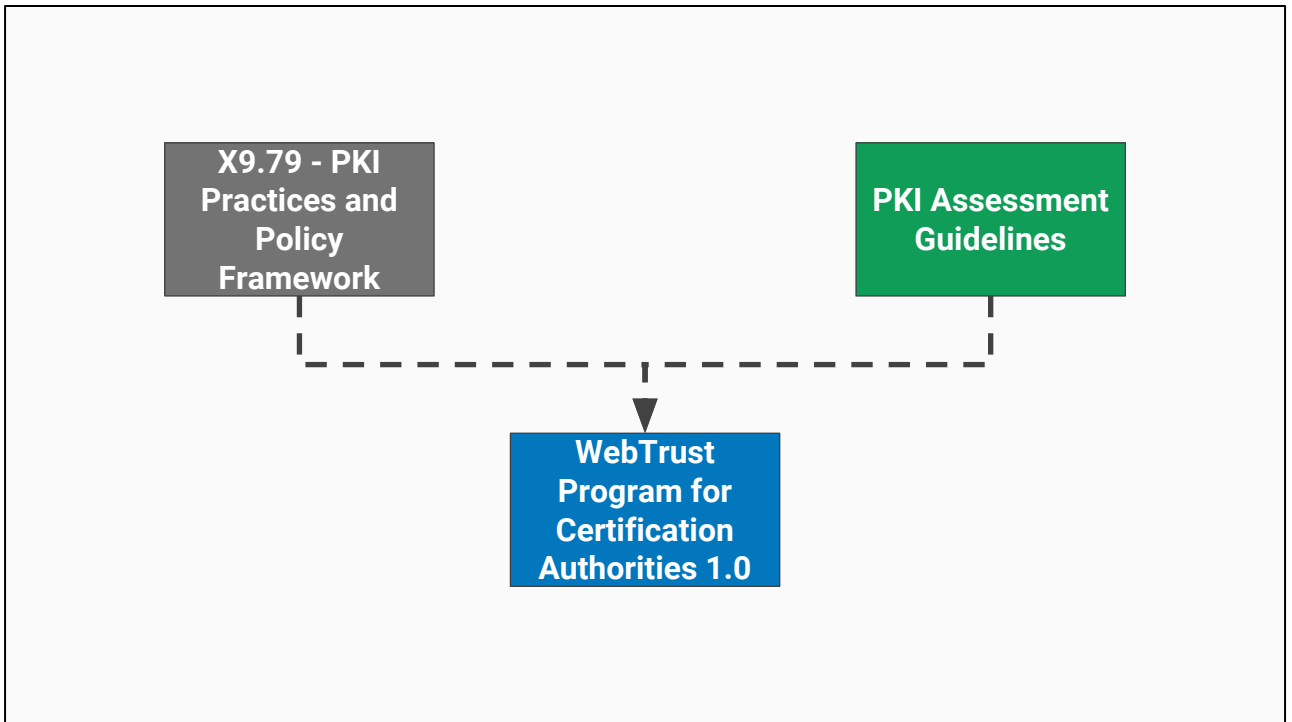
- Addressing assessment controls and criteria
- Work edited by Mark Lundin at KPMG (Source: <https://www.prc.gov/docs/61/61337/081031%20IAC%20motion%20to%20PRC-corrected.pdf> , <https://www.ietf.org/mail-archive/web/pkix/current/msg23894.html> )
- Annex B established many of the CA Control Objectives ( [http://www.oasis-pki.org/pdfs/CA\\_Trust.pdf](http://www.oasis-pki.org/pdfs/CA_Trust.pdf) )
- Published: 2000

**X9.79 - PKI  
Practices and  
Policy  
Framework**

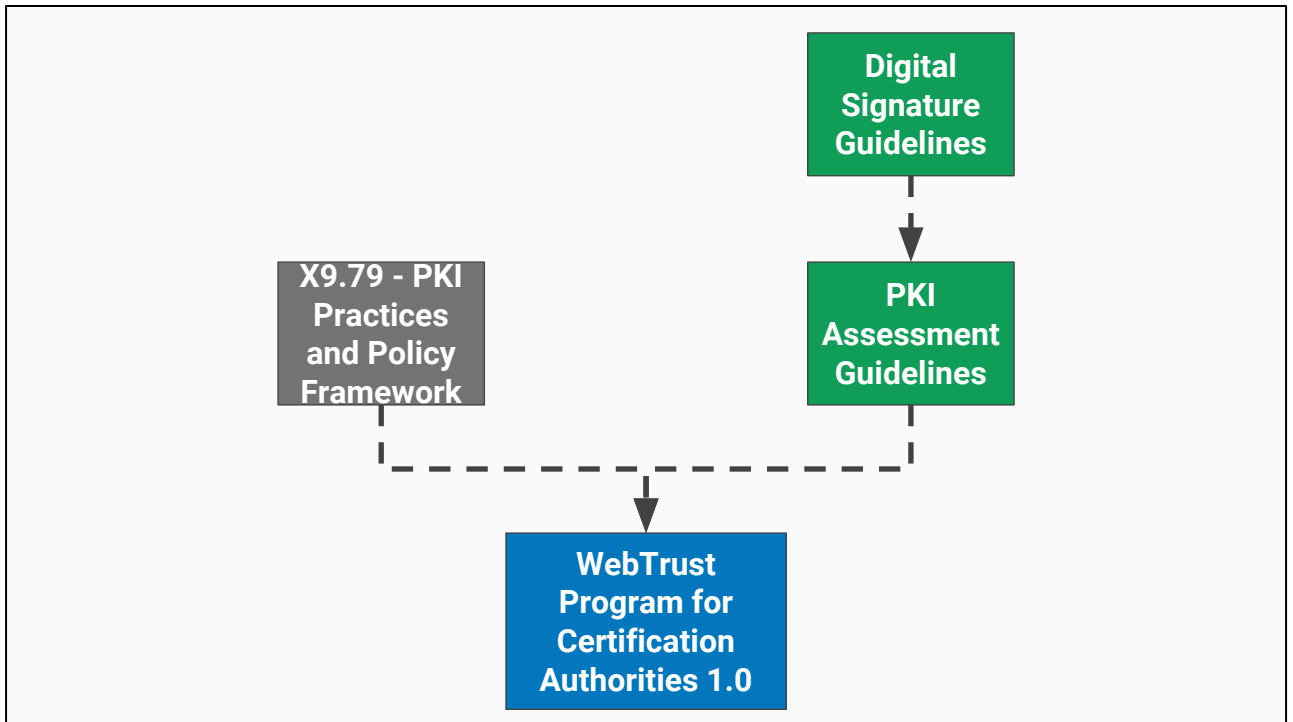


**WebTrust  
Program for  
Certification  
Authorities 1.0**

- Published: 2000
- WebTrust incorporated feedback from the draft X9.79 and set out criteria that can be used to perform audits under professional auditing standards
- At the time of WebTrust, there existed a variety of assessment criteria and audits. For example, some frameworks for digital signatures used SAS 70 audits (but we'll get back to that)
- Source: <http://www.webtrust.org/homepage-documents/item65306.pdf>



- WebTrust for CAs didn't just borrow from X9.79, it had other sources that it considered and was inspired by
- One of these was the American Bar Association's PKI Assessment Guidelines (Source: Page 9 of <http://www.webtrust.org/homepage-documents/item65306.pdf> )
- Borrowed From / Harmonized With / Inspired By / Related To are going to be used interchangeably throughout
- If X9.79 looked at what the goals of CA operations are, the PAG looked at the set of legal framework and concerns and (to a lesser extent) what are things to be looked for that would mitigate or address those concerns
- These weren't the only documents going around (see [http://www.americanbar.org/content/dam/aba/administrative/science\\_technology/sabett.ppt](http://www.americanbar.org/content/dam/aba/administrative/science_technology/sabett.ppt) or <https://www.enisa.europa.eu/events/eid-workshop/proceedings/02-02-DigiCert/view> )



- I can't mention the PAG without also mentioning the preceding effort of the ABA's Digital Signature Guidelines, which looked at this in the context of legal signature recognition. The PAG is not a direct descendent of this effort, but inspired by and builds upon.
- Also, fun note about the PAG - there was recognition that evaluating a bunch of different CP/CPS and consistency between them would be rather difficult. They strongly endorsed the adoption of machine readable structure to CP/CPS and developing documentation from that - in this case, XML was all the rage.

**X9.79 - PKI  
Practices  
and Policy  
Framework**



**ISO 21188**

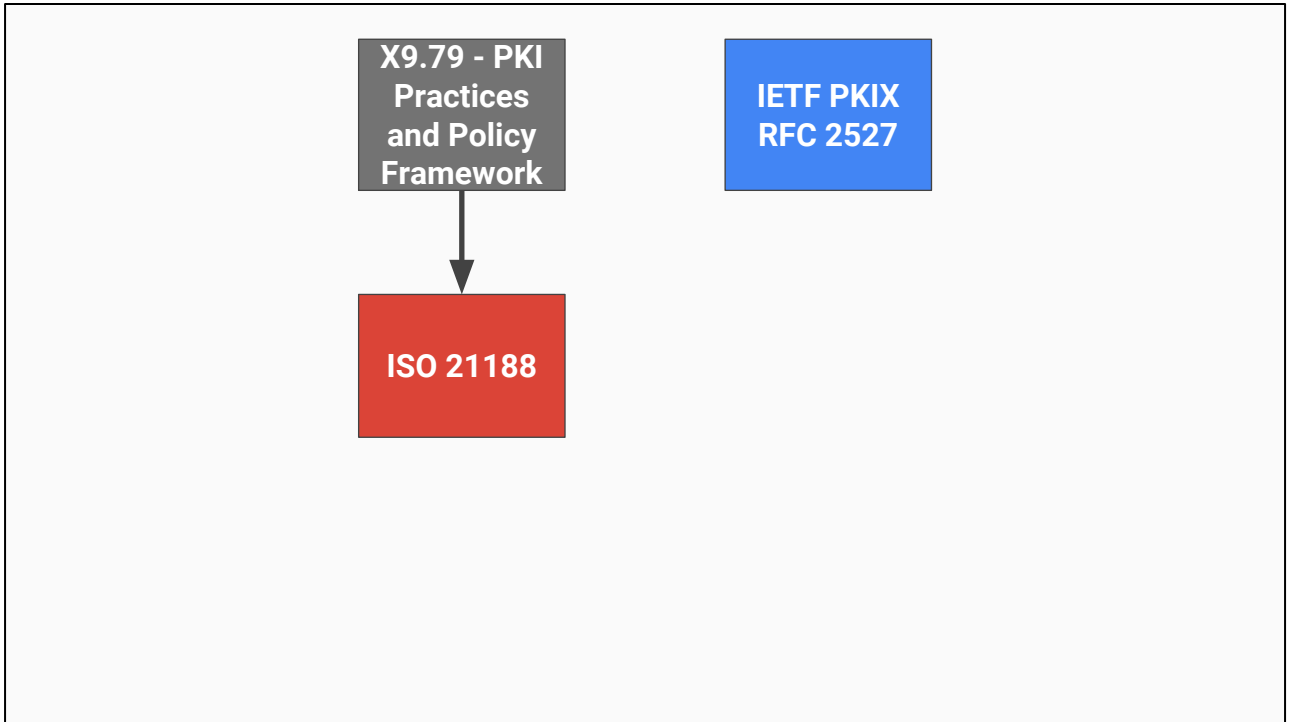
- Now I mentioned that X9.79 was a common ancestor, and so I'm going to switch a little to speak about the parallel development of the ETSI assessments
- X9.79 was adopted by ANSI and subsequently brought to the international set of standards as ISO 21188
- The focus on 21188 was primarily about assessments in the context of financial services - reflecting its origins and basis in the American Bankers Association's needs
- ISO 21188 was part of the TC68 effort (standards for financial services)

Source:

[https://cdn.ymaws.com/www.issa.org/resource/resmgr/JournalPDFs/PKI\\_Under\\_Attack\\_ISSA0313.pdf](https://cdn.ymaws.com/www.issa.org/resource/resmgr/JournalPDFs/PKI_Under_Attack_ISSA0313.pdf)

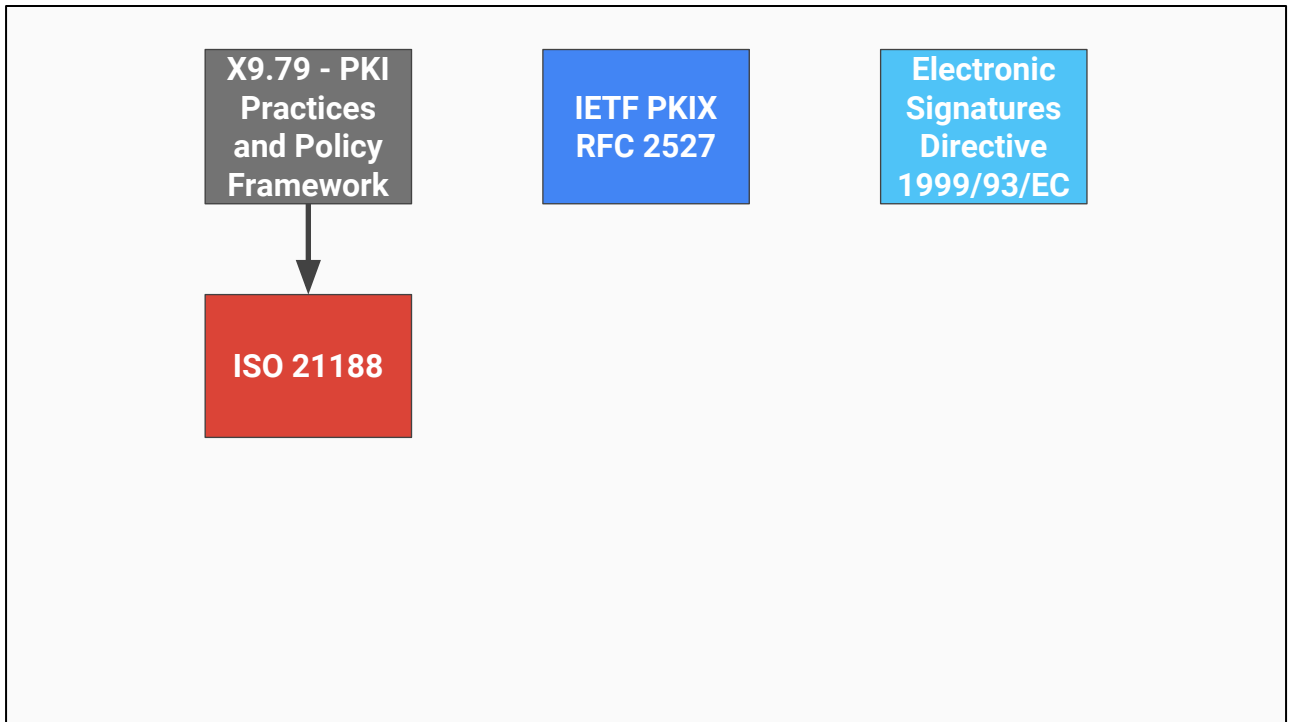
Source:

[https://www.etsi.org/deliver/etsi\\_tr/102000\\_102099/102040/01.02.01\\_60/tr\\_102040v010201p.pdf](https://www.etsi.org/deliver/etsi_tr/102000_102099/102040/01.02.01_60/tr_102040v010201p.pdf)



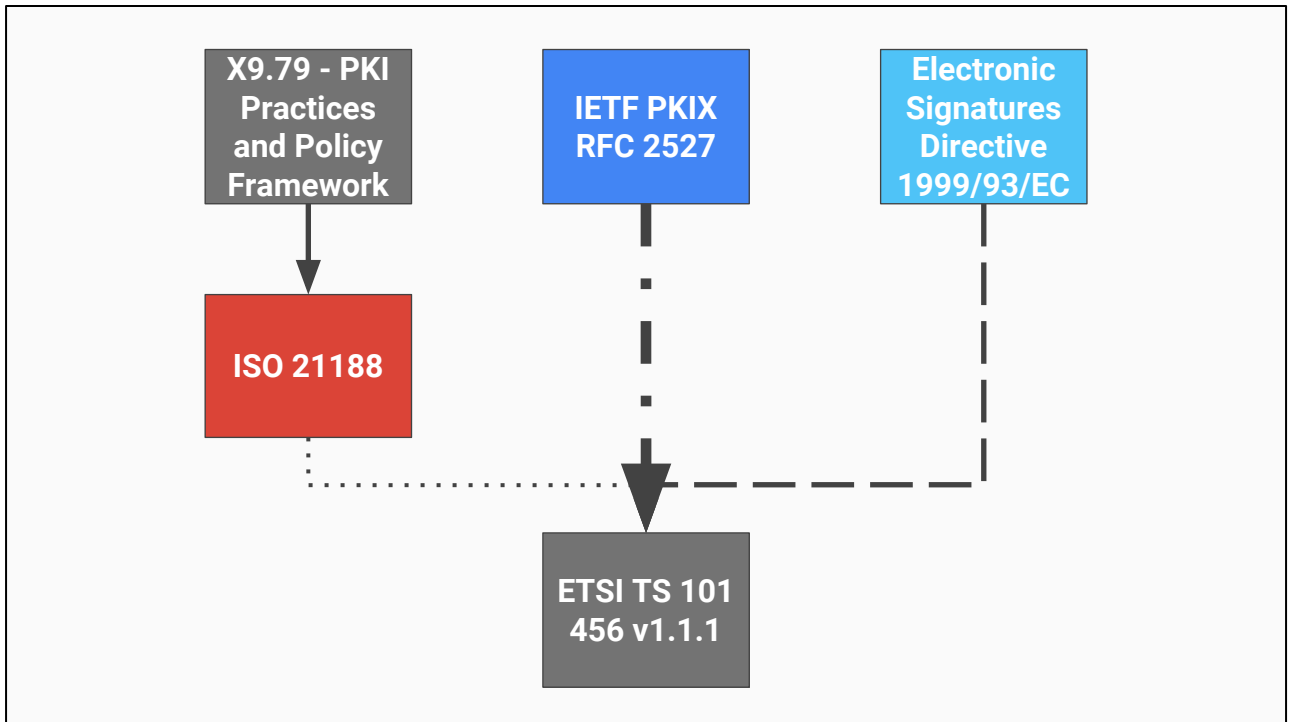
- While this activity was going on, the IETF PKIX WG was developing RFC 2527, which, with some similarities to the PKI Assessment Guidelines and X9.79 activity, looked at structure for CP and CPS to ensure consistent and clear documentation was included

Source: <https://tools.ietf.org/html/rfc2527>



- Also in the midst of all this activities, the EU Commission published the Electronic Signatures Directive 1999/93/EC that attempted to harmonize cross-border recognition of certificates, particularly for legal purposes
- This is not audit criteria or requirements, but does speak to the general framework and needs that need to be addressed

Source: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999L0093>



- These three documents all contributed to the development of ETSI TS 101 456
- 101 456 was harmonized with ISO 21188 - 21188 was focused on financial services, 101 456 wanted to be more general for services
- Framework for 101 456 was borrowed from RFC 2527
- Goal of 101 456 was to address the goals and expectations setup in the ESD
- We'll discuss audit methodology separately; 101 456 focused on policy expectations - it didn't look at how to measure and assess

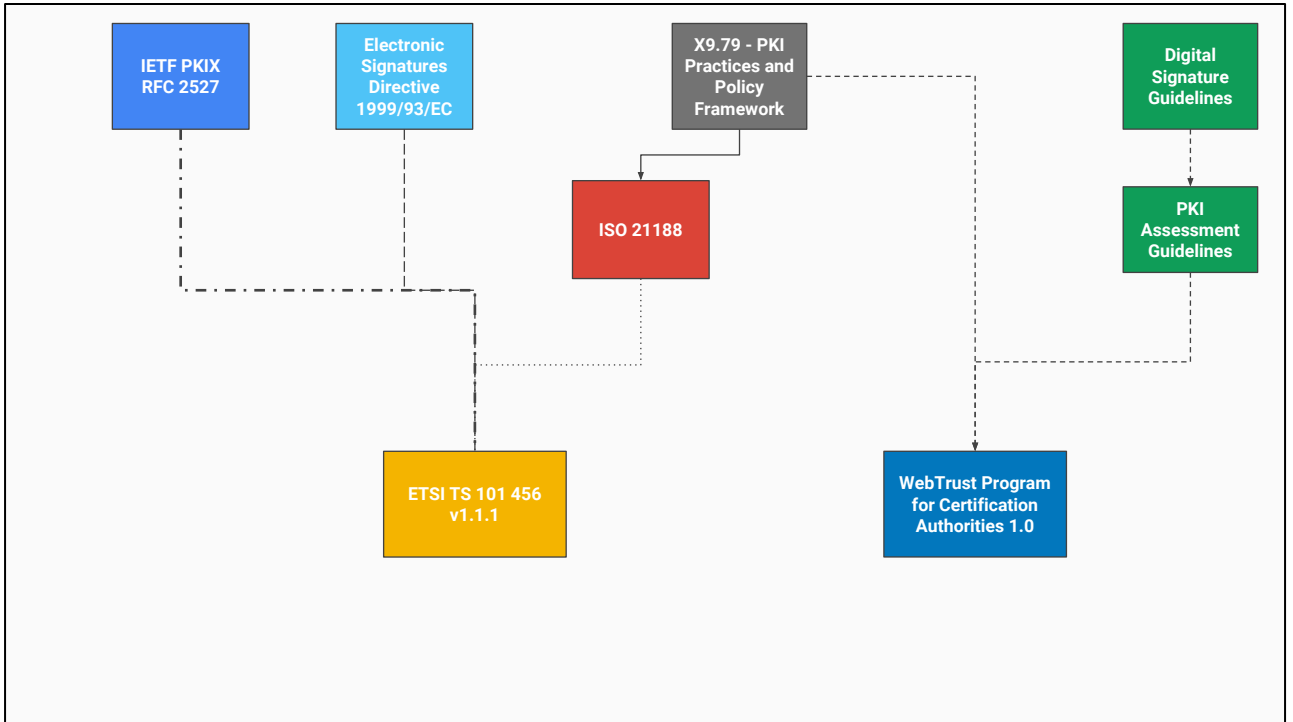
Source:

[https://www.etsi.org/deliver/etsi\\_ts/101400\\_101499/101456/01.01.01\\_60/ts\\_101456v010101p.pdf](https://www.etsi.org/deliver/etsi_ts/101400_101499/101456/01.01.01_60/ts_101456v010101p.pdf)

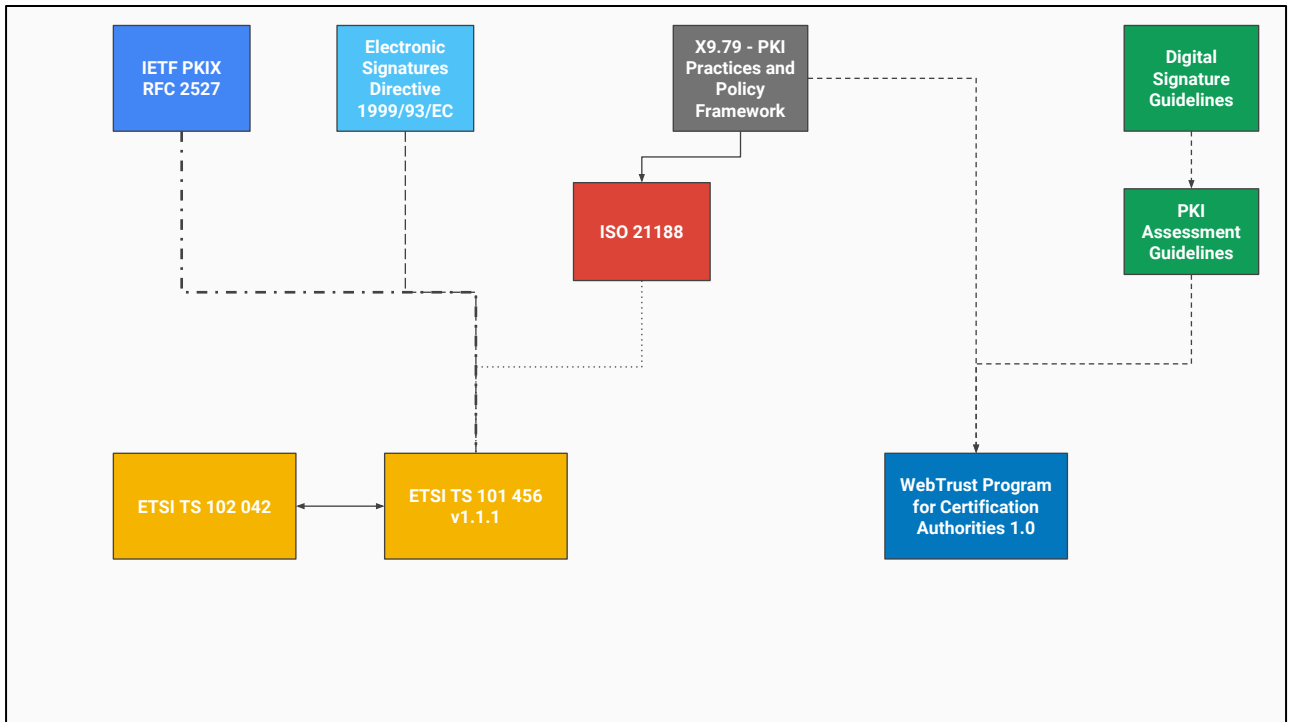
Source:

[https://www.etsi.org/deliver/etsi\\_tr/102000\\_102099/102040/01.02.01\\_60/tr\\_102040v010201p.pdf](https://www.etsi.org/deliver/etsi_tr/102000_102099/102040/01.02.01_60/tr_102040v010201p.pdf)





- Big Picture View: How did the various criteria emerge



- While TS 101 456 was about meeting the objectives of the Electronic Signatures Directive, TS 102 042 more broadly expanded this to cover other types of certificates (non-qualified)

# Audit Standards

- I'm going to take a quick detour here - I've been talking about how the audit criteria were written and what was feeding into this effort, but it's equally important to take a look at the audit standards - how are these criteria used and evaluated, what's expected of auditors and assessors, and how are the audits performed.
- You may be thinking, at this point, "I've gone through more audits than years you've been involved in PKI" - and that might be true, but I'm also willing to bet that I've probably had to consume more audit reports than everyone but the auditors in the room.
- This is not a complete summary of the audit standards used. The world is big and the time is short, so it's not going to try to look at how every standard evolved. My goal is to hit the high points, give pointers to things that are related (but not identical), so that we can have an approximate understanding of what's trying to be done.
- Relevance: The questions about what should an audit report contain, what should it examine, how should it be produced, and what are the limitations are directly addressed by this.

WebTrust



SAS70

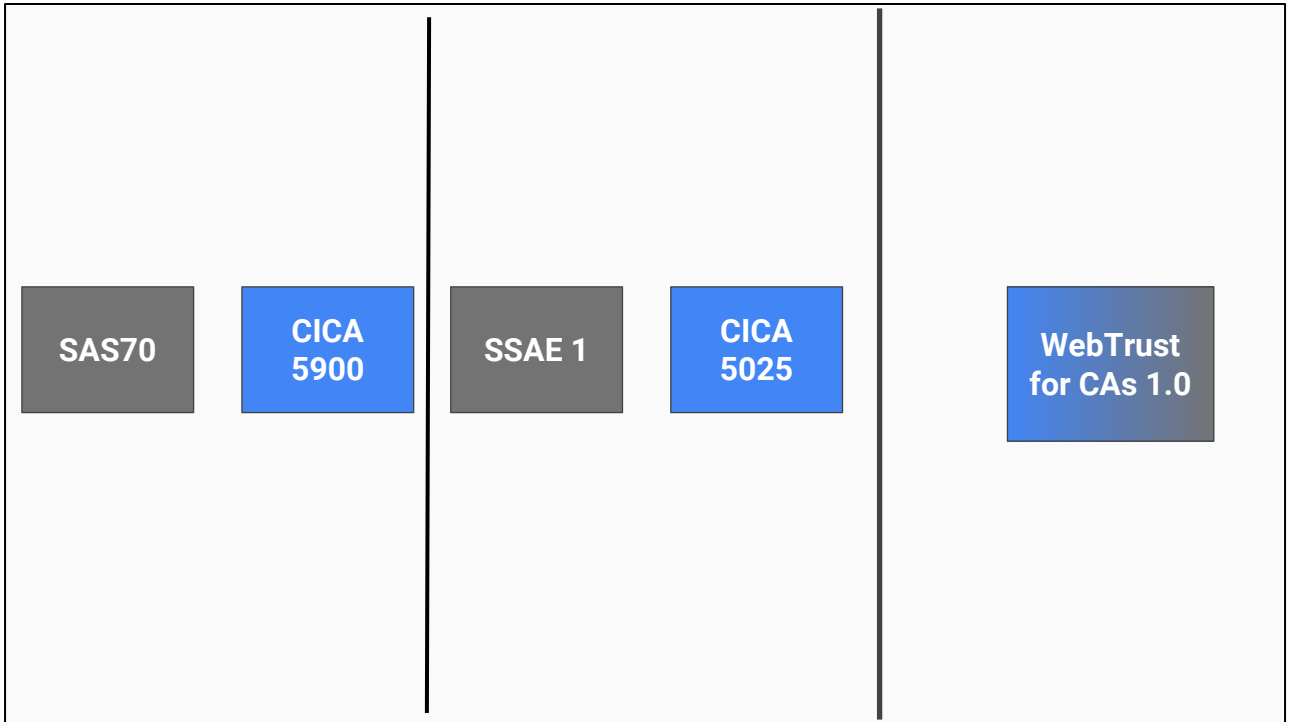
CICA 5900

- One of the things you see in the early work - whether the ABA PAG or related work - is a distinction being made between assessments and audits, and who are the parties that might perform these.
- The PAG explores a variety of approaches in the context of the US legal structure - and particularly in the context of defining and reducing liability for CAs and their PKIs. These structures looked at the independence of the party performing the assessment, the use of consistent criteria, etc. While it looks at the possibility of evaluation from a variety of parties, one early 'winner' was AICPA/CICA with the development of WebTrust.
- Why WebTrust? PAG had examined a variety of ways of conducting assessments, and who might conduct them. At the time, PKIs were being assessed using various criteria (either in-house or nascent criteria that would become those audit standards), "according to" notions like SAS70 or CICA 5900
- SAS 70 / CICA Section 5900 aren't for this purpose (financials, auditor to auditor), WebTrust evolved to meet that need

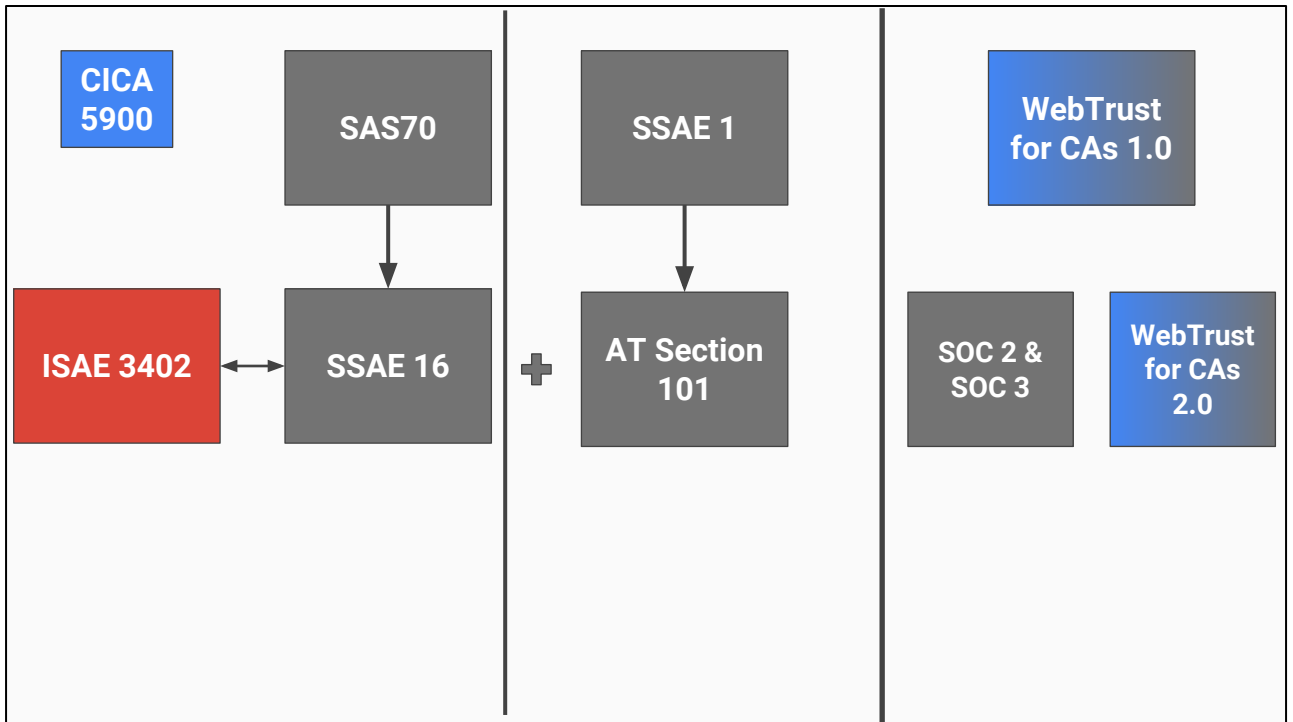
Source: <http://sas70.com/FAQRetrieve.aspx?ID=33286>

Source: [http://www.oasis-pki.org/pdfs/CA\\_Trust.pdf](http://www.oasis-pki.org/pdfs/CA_Trust.pdf)

Source: "Security without Obscurity: A Guide to PKI Operations", Jeff Stapleton, W. Clay Epstein, 9.9 "PKI Compliance"



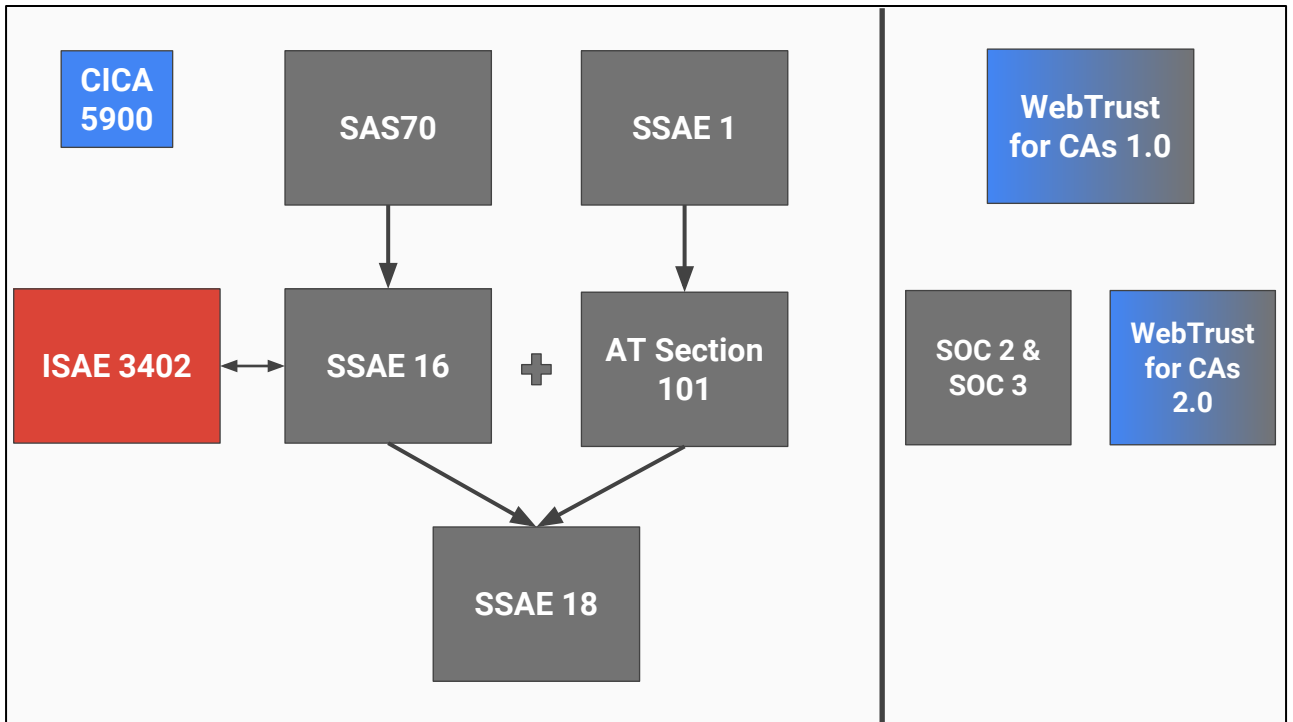
- SAS 70 / Section 5900 were about financials, but included sections about “service organizations” - for purposes of financial controls
- SSAE 1 / CICA 5025 set up attestation standards and principles more broadly



- SAS 70 was covered under AU 324 - about internal control over financial reporting
- SAS 70 mentioned service organizations, hence why folks had used it
- In 2009, IAASB released ISAE 3402, which is about reporting on controls at service organizations
- In 2010, AICPA updated and replaced SAS 70 with SSAE 16 (about financial controls) and AT Section 101 (attestation standards, addresses the non-financial use case)

Source:

[https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/faqs\\_service\\_orgs.pdf](https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/faqs_service_orgs.pdf)



- In 2016, SSAE 18 was published
- SSAE 18 reharmonizes the previous SSAEs, leads to new renumbering of the relevant standards (for the US)
- While all of this is going on, similar work is going on internationally (CICA -> CPA Canada, CICA 5900 -> CSAE 3000 (July 2015), ISAE 3000, etc
- WebTrust Illustrative Reports - Published 2017

Source:

<https://www.mnp.ca/SiteAssets/media/PDFs/APSG/New%20and%20Proposed%20Changes%20to%20Assurance%20Sections%20for%20the%20Two%20Years%20Ended%20September%2030%202016.pdf>



ETSI

**ETSI TS 101 456**  
**v1.1.1**

CWA 14172-2

CWA 14167-1

ETSI TS 101 456  
v1.1.1

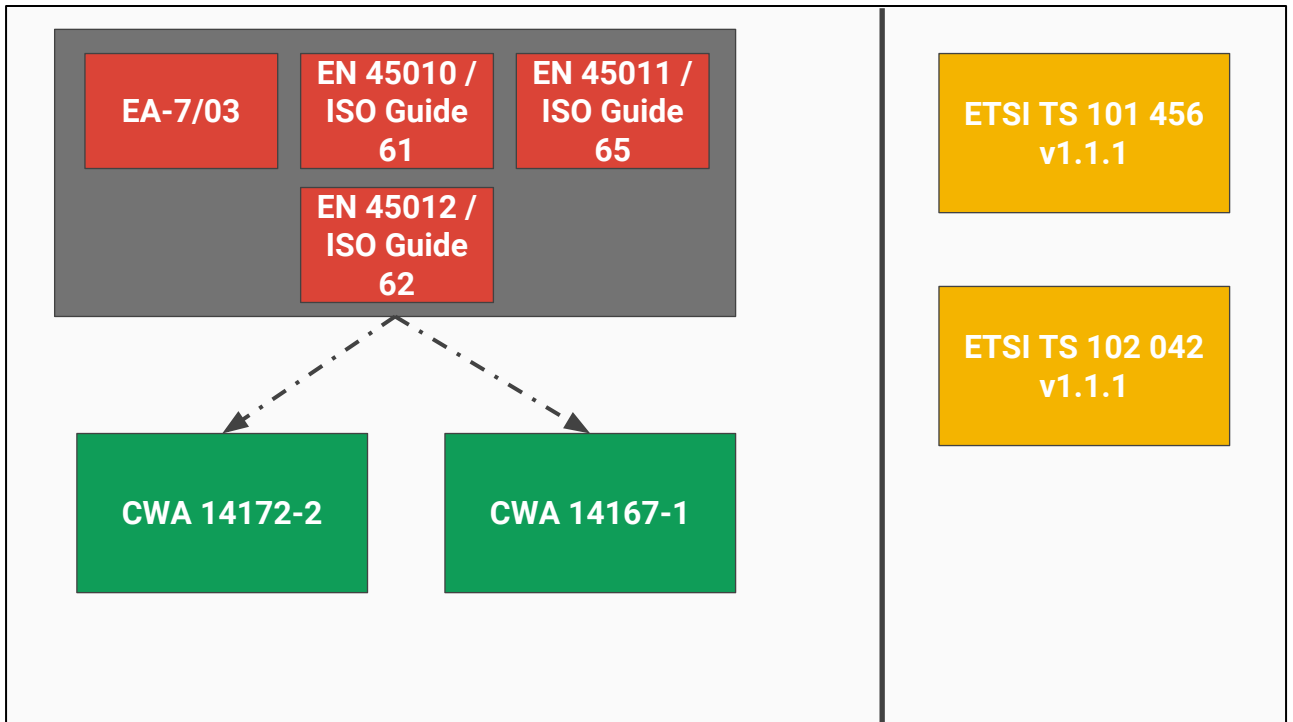
ETSI TS 102 042  
v1.1.1

- EESSI was created by the EC as a joint effort between CEN/ISSS and ETSI/ESI to develop a set of standards relevant to the Electronic Signature Directive
- The CWA documents were the result of these joint meetings
- Note: At the time of the Signature Directive, it was a voluntary scheme of accreditation; no rules existed yet
- While 1999/93/EC was a single release, operational guidance (“Commission Decisions”) were provided throughout the lifetime that built upon the activities in the standards space to establish more explicit relationship between the standards and the Signatures Directive
- One of the first outputs of that was CWA 14172-3 / 14172-2. In context, it’s similar to the assessment of the PAG - it talked about the general principles about assessments and how they should be done, but set objectives rather than specific requirements (it was non-binding)
- Another output was CWA 14167-1, which was about system security requirements for CAs. It was similar to WebTrust for CAs - it was an enumeration of criteria/objectives and ways to meet them.

Source: <https://neytendastofa.is/lisalib/getfile.aspx?itemid=947>

Source: <https://www.dnielectronico.es/PDFs/cwa14167-01-2003-Jun.pdf>

Source: [https://en.wikipedia.org/wiki/Electronic\\_Signatures\\_Directive](https://en.wikipedia.org/wiki/Electronic_Signatures_Directive)

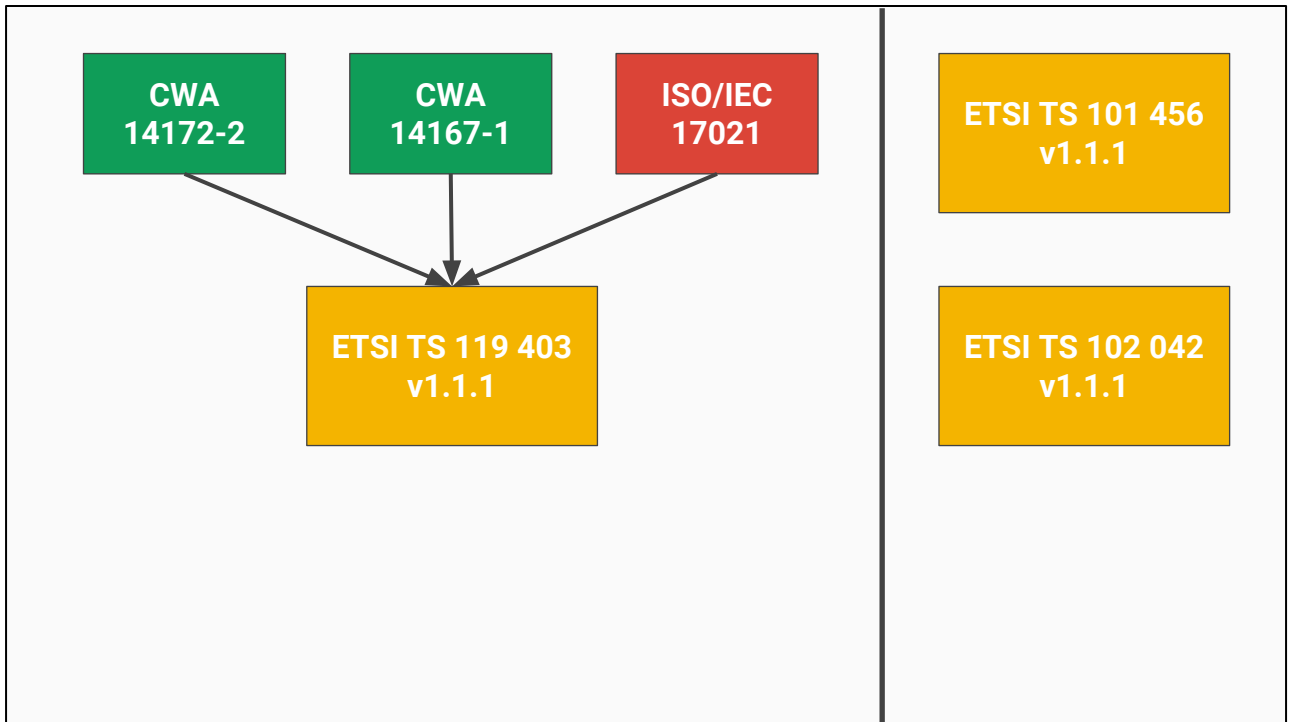


- The framework for these assessments had professional standards applicable - some which were European Norms based on ISO standards, others based local professional rules
- Set up the framework for understanding how to perform these evaluations - a variety of options that varied based on national schemes and expectations

Source: [https://adgrafics.net/docs/other/etsi\\_ts\\_119403v010101p.pdf](https://adgrafics.net/docs/other/etsi_ts_119403v010101p.pdf)

Source:

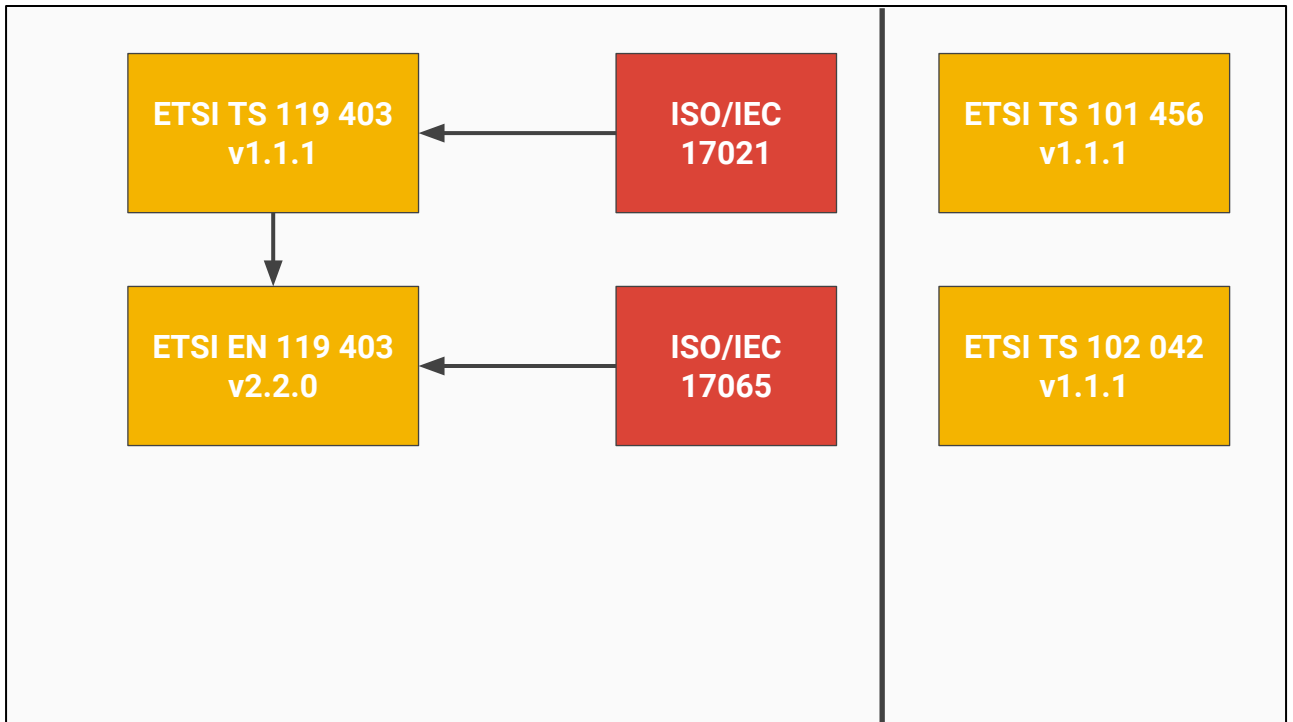
<https://cabforum.org/mailman/private/management/2009-October/002371.html>



- These documents laid out principles, and met some of the objectives, but there wasn't a consistent cross-country recognition scheme
- Regulation (EC) No 765/2008 tasked EA (<http://www.european-accreditation.org/>) for purposes of establishing National Accreditation Bodies to facilitate cross-border accreditation schemes
- Following this, ETSI looked to normalize how assessments are conducted - supplanting the CWA documents with an interoperable framework based on ISO 17021

Source:

[https://www.enisa.europa.eu/publications/tsp\\_standards\\_2015/at\\_download/fullReport](https://www.enisa.europa.eu/publications/tsp_standards_2015/at_download/fullReport)



- During the development, the decision was made that it's easier to fit 17021 into 17065 than it is to fit 17065 into 17021, so it was updated to be based on 17065
- Incorporated elements from 27001 / 27006

Source:

[https://www.enisa.europa.eu/publications/tsp\\_standards\\_2015/at\\_download/fullReport](https://www.enisa.europa.eu/publications/tsp_standards_2015/at_download/fullReport)  
( 2.1.2)

Putting it all  
together

## ETSI

- Certification scheme - Examining whether a given system, product, or process faithfully implements what is required.

## WebTrust

- Attestation audit - Examining historic data and offering an opinion about management's presentation of / statement of facts and details based upon defined criteria.



## ETSI

- The output is a certificate - If the TSP meets the criteria (or has a contractual agreement to meet the criteria within 90 days, if they aren't yet), they get a certificate. Based upon specific requirements being looked at and met.

## WebTrust

- The output is an opinion - Either on the subject matter itself or the CA's management's assertion, about whether or not, in the auditor's opinion, the facts are fairly stated, based on the principles and criteria used to evaluate the claims or evidence.

## ETSI

- Certifications are based on ISO/IEC 17065, as expressed in ETSI EN 319 403

## WebTrust

- Audits are conducted (broadly) against the ISAE 3000 framework, as adapted for individual countries and bodies (e.g. AICPA + AT-C 205, CPA Canada and CSAE 3000, etc)

## ETSI

- Assessors (CABs) have to meet the requirements of ETSI EN 319 403. Reporting requirements are specific to the certification scheme, and may be adjusted as necessary (e.g. TS 119 403-2)

## WebTrust

- Assessors (auditors) have to comply with their own professional standards body (AICPA, CPA Canada, etc), which are generally based on international standards (e.g. IFAC ISAE 3000). Reporting is defined by professional standards and is restricted in various ways.

## ETSI

- The assessment criteria (e.g. ETSI EN 319 403 and ISO/IEC 17065) sets requirements such as what the auditor must consider or examine. Based on review of evidence that demonstrates compliance - both procedures and historic evidence

## WebTrust

- The professional standards (e.g. AICPA AT-C 105) sets requirements such as what the auditor must consider. Based on building (reasonable) confidence that every statement matched by criteria is "fairly stated"

## ETSI

- Defines “problems” as non-compliance. The CA is expected to report any (pending or executed) changes, and if the changes would make it non-compliance, the CAB takes steps to resolve

## WebTrust

- Defines “problems” as misstatements, which may be material and pervasive, or potential misstatements based on lack of evidence.

## ETSI

- Non-compliance may be resolved by suspension or termination of certification, or may be resolved by contractually-guaranteed corrective action to be taken to get back into compliance, potentially with additional supervisory audits.
- Ternary State - Certified, Not Certified, Passed with pending nonconformities

## WebTrust

- Misstatements are resolved by expressing qualifications on the opinion; except for those explicitly identified misstatements, management fairly stated things.
- Binary State (ish) - Unmodified or Modified (Qualified, Adverse, Disclaimer)

## ETSI

- Process: Examine system design and processes. Evidence is gathered to make sure the design is consistent with each individual “Requirement” by the compliance scheme.

## WebTrust

- Process: Gather historic evidence over a period of time (bounded on the minimum and maximum by professional standards) to demonstrate that each “Principle” and “Criteria” has been met.

## ETSI

- Primarily focused on present (compliant) and future (all changes are still compliant), with (some) historic evidence used to match statement with practice

## WebTrust

- Primarily focused on past - Can we get enough proof (based on the criteria) to determine whether or not management did what they said they did, when they said they did it.



## ETSI

- Scope: Focused on the organization and system. Borrows heavily from ISO 27xxx framework for system assessment, about institutional controls and practices

## WebTrust

- Scope: Focused on the specific statements and claims being made. Developed with the specific notion of individual root certificates (CAs), as operated by organizations (management)

## ETSI

- Scope: Organization (TSP) is the root of the assessment. The assessments holistically consider the organization and any CA certificates they may operate.

## WebTrust

- Scope: PKI hierarchy - rooted in a CA (certificate) - is the root of the assessment. How that Ca works is supported by the organization's (management's) claims.

- The WebTrust notion of CA borrows from the IETF PKIX notion of CA, combined with the X9.79 statements about CA.
- The ETSI notion of "CA" is about equivocating it as a "Trust Service Provider" (TSP), the organization operating things. ISO/IEC 17065 and the incorporation of/inspiration by ISO/IEC 27001/27002/27006 are about looking at the organization and how they manage the controls for an abstract system.

## ETSI

- As of Date X, System was certified Compliant with Scheme. Compliance is determined based on examining evidence from Dates Y-Z. No minimum ranges specified, maximum range specified by scheme (319 403 = 2 years, TS 119 403-2 = 1 year). If something changes, certification may be revoked.

## WebTrust

- Type 1: On Date X, reasonably confident that management designed and implemented correctly, but didn't test whether it actually works.
- Type 2: On Date X, based on examination of Dates Y-Z, reasonably confident that management did what they said they would, and that's consistent with what they should.

Agenda

## Agenda

- Background
- Motivation
- History
- **Current Issues**
- Potential Solutions

# Terminology

Now armed with this historic context, we can start to take a better look at the terminology we have, what might have been meant or desired, and why that may not actually be working as intended

# “Performance Audit”

- CA/Browser Forum Bylaws, v2.1, § 2.1 (b)(6)
- Problem: For AICPA/CPA Canada/etc, has a very specific definition, and isn't related to WebTrust (it's about Government Auditing)
- Problem: For ETSI, doesn't even have a possible interpretation - ISO/IEC 17065 describes a certification scheme
- Probable Goal: “You're actually issuing certs and having historic evidence examined”

That said, there's another bug here worth mentioning - we talk about “properly-qualified” auditor, but that's a loan-phase from the BRs that doesn't map to the Bylaws anymore, since that's just one CWG's definition (The SCWG). “Licensed” might work for WebTrust, but not for ETSI. “Accredited” might be closer, except WebTrust / CPA Canada is not accrediting auditors - they're licensing the brand.

# “Point in Time Readiness Assessment”

- Baseline Requirements, v1.6.0, § 8.1 ¶3
- Terminology in the BRs was “loaned” from the EVGs and its early drafts
- Concept introduced by Don Sheehy in 2006 in Mountain View F2F
- The concept of “EV Readiness Audit” was a thing that existed in assessing the draft EVGs vs the Final EVGs, and was about how to bootstrap trust with a new certificate policy when no existing CAs were actually issuing against it, and thus couldn’t provide evidence?
- Problem: Doesn’t match 1:1 to WebTrust concept under ISAE 3000 (and related AICPA/CPA Canada issues)
- Problem: ETSI certification doesn’t remotely have the concept. An evaluation against ISO/IEC 17065 or ETSI EN 319 403 is supposed to consider operational evidence
- Probable Goal: “Your systems should be compliant, once you actually start using them”

Source: <https://cabforum.org/mailman/private/management/2006-July/000148.html>

Source:

<https://www.mail-archive.com/dev-tech-crypto@lists.mozilla.org/msg02679.html>

# “Period of Time”

Mozilla Root Store Policy, v2.6.1, § 3.1.4

- Concept comes from SAS 70 / SSAE 16 / AT 101 / SSAE 18 concept of Type 1 and Type 2 reporting
- Problem: ISO/IEC 17065-based certification schemes don't have this conceptual split. You're certified or not certified. How much evidence is going to be examined is left up to scheme requirements and the continuous evaluation by the CAB (because of contractual reporting requirements)
- Probable Goal: “You did what you said you do, and someone else confirmed.”



# “Key Ceremony Report”

Baseline Requirements, v1.6.0, § 6.1.1.1 ¶1

- Concept introduced in the first drafts of the EV Guidelines, carried into the first drafts of the BRGs
- Problem: Inherits from WebTrust concept based on attesting opinions about facts, leaving limited room for ETSI reporting on compliance with criteria
- Problem: Unclear (in text) who the intended consumer is - public or auditor - and thus applicable professional standards or expectations about documents
- Probable Goal: Public documentation of compliance & provenance

Source:

[https://cabforum.org/wp-content/uploads/EV\\_Certificate\\_Guidelines\\_draft11.pdf](https://cabforum.org/wp-content/uploads/EV_Certificate_Guidelines_draft11.pdf)

Source:

[https://cabforum.org/wp-content/uploads/Baseline\\_Requirements\\_Draft\\_30b.pdf](https://cabforum.org/wp-content/uploads/Baseline_Requirements_Draft_30b.pdf)

# “Currently Valid Audit Report”

Baseline Requirements, v1.6.0, § 8.1

- Introduced in EVGs drafts (e.g. Draft 11, § J, 35(a)(1)), tied specifically to WebTrust Seal (not Report), carried over to the BRs
- Problem: WebTrust Seals are valid / expired / suspended, reports are not. Validity of reports is thus unclear.
- Problem: ETSI notion of certification allows for non-conformities to be in the process of being resolved, at-or-after the issuance of the certificate
- Probable Goal: If you don't have (enough) evidence in practice, you can still get a report sufficient to get into programs, so that you can generate evidence and get a retroactive certification/attestation report.

Source: <https://cabforum.org/mailman/private/management/2006-July/000148.html>

# “Qualified Audit”

- Problem: Mozilla (and earlier BRs and EVGs) seemingly refer to the WebTrust model, which is an expression of a modification of opinion based on certain qualifications to be addressed.
- Problem: Microsoft seemingly refer to it to mean “Suitable Audit”
- Problem: ETSI, as a certification scheme, fundamentally doesn’t express qualifications. Non-compliance and non-conformities may or may not be identified and may or may not be remedied by the time of certification
- Probable Goal: Any testing procedures that failed, any controls or criteria that weren’t met, are clearly documented, explained, and remediation planned

Source:

[https://www.etsi.org/deliver/etsi\\_en/319400\\_319499/319403/02.02.02\\_60/en\\_319403v020202p.pdf](https://www.etsi.org/deliver/etsi_en/319400_319499/319403/02.02.02_60/en_319403v020202p.pdf) 7.6

# Expectations

However, there's also a more existential problem. If the whole point of that long history lesson earlier in this presentation was just to nit-pick on certain misused terms, then it was an excellent soliloquy, but not a productive one. No, the meta-goal of this presentation is to examine how we, as an ecosystem, are pretty good at wanting X, saying Y, and getting Z - and disappointing everyone who expected X or actually did Y, whether they be a CA, an Auditor, a Browser, or a Relying Party. That's the real "current problem"

# L.R.E.A.M.

“Liability Rules Everything Around Me”

As the PKI Assessment Guidelines go into (at great length), one of the core concerns when those documents were being developed and PKI envisioned was about liability. Subscriber and Relying Party Agreements are about getting these parties to agree to Liability. The CP/CPS is about disclaiming liability. The audit/attestation/certification is about reducing the liability from (including the root, trusting the CA, integrating the PKI, using the cert).

While this may sound a very US-centric view, the development of the Electronic Signatures Directive, and ultimately eIDAS, in part was about bringing strong identity into the space, making it have constitutive (legal) value, with clear expectations about when you can shed liability (e.g. non-repudiation, certification).

Our model of the PKI is not necessarily based on trust, it's about liability - I'll trust you, but only if it's not my fault if things go wrong.

# Reducing Risk for Browsers

- The original adoption of audits as a framework was largely lead by Microsoft, in 2001, with the adoption of and recognition of WebTrust for CAs
- Prior to that, the approach taken was one similar to Netscape - Convince us and pay us (At the time, \$150K for Netscape inclusion)
- Microsoft was concerned about liability. It's not to say Mozilla wasn't, but as Frank Hecker explained, liability is a consequence of failures of security, and the high-order concern is about security.
- Additionally, Frank's expectations were focused on transparency - the audit may not be the most valuable thing, especially if the CA is transparent about its controls and operations

Just because we started with liability doesn't mean liability is the goal. As Microsoft would later update the root program to note, there's a desire to have better criteria and better approaches, to better reflect the security goals, and not just the perceived legal goals.

Source:

<https://web.archive.org/web/20080906214557/https://technet.microsoft.com/en-us/library/cc751157.aspx>

Source: <http://hecker.org/mozilla/ca-certificate-metapolicy>

Source: <https://cabforum.org/mailman/private/management/2006-July/000148.html>

Source:

<https://groups.google.com/d/msg/netscape.public.mozilla.crypto/xhulOmyZpn8/RJP4kLZ9eNIJ>

Source:

<https://web.archive.org/web/20040412221430/http://hecker.org/mozilla/ca-certificate-faq/policy-details/>

# Reducing Risk for CAs

- While CAs may have originally been invested in audits to reduce risk and liability - as the PAG discusses - the current schemes aren't necessarily helping that.
- If a CA partners with an RA, do they have enough detail about that RA's operations? Do they have the skill and expertise to consume the audit and its implications (as appropriate to the scheme and report)? As WebTrust for RAs drafts note, there's a real need and opportunity to improve this.
- How much confidence should a CA require before cross-signing another CA? One of the arguments against "Super-Roots" is that schemes based on audits alone don't really provide the necessary confidence - that's why you have activities in Mozilla like public review, precisely because it was expected that audits would be inadequate for trust, and perhaps even entirely unnecessary.
- How can a CA increase its confidence that it's not going to get booted by a root program? How can audits help build in that safety and routine assessment, so that they don't get surprised by that one bad day when their whole PKI gets excised?



# Reducing Risk for Users

- The evolution of audits in the WebTrust-based space, borrowing from X9.79 and the ABA PAG, was about shifting the liability to the user and relying party. The assessment would just tell the user what they said they do and how they claim to do it, and the independent audit attestation would give some confidence that it's fairly stated.
- However, the user was then expected to examine the RP agreement, the CP, the CPS, the PDS, and any other supporting documents to individually, for every certificate and use, make a decision whether or not to trust it. The responsibility was all on them, and as a result, so was the liability.
- Thus, audits aren't a means to reduce liability of users - it increases it. Relying on an audit to tell you a CA is trustworthy is misusing the system!

Agenda

## Agenda

- Background
- Motivation
- History
- Current Issues
- **Potential Solutions**