Firma digital trasfronteriza, la experiencia europea

Santiago, 27 de junio de 2019

Laura Cabezas

- **Directiva de firma 1999/93/CE**
  - Firma electrónica como medio de identificación del firmante.
  - Transposición.

Marco legal actual

Reglamento eIDAS (UE 910/2014)

Contempla legislación de desarrollo para los aspectos técnicos:

2 áreas:

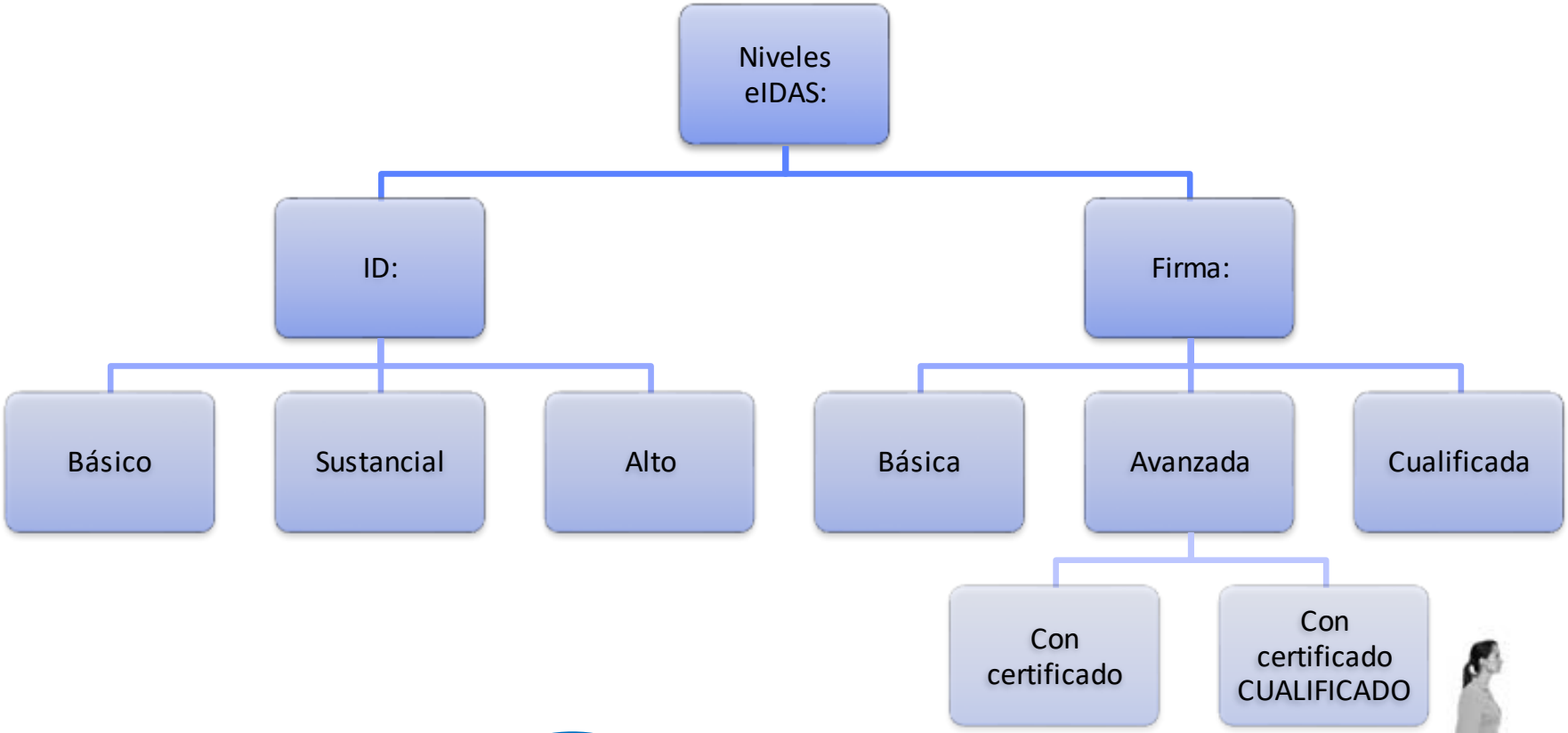
Decisiones de ejecución

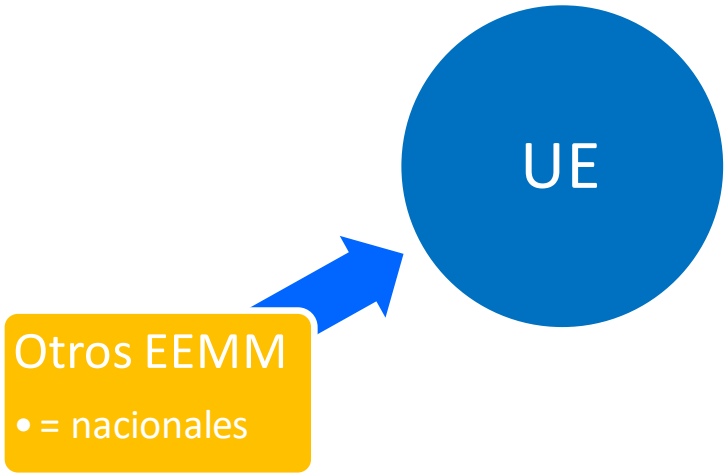
Normas Europeas ETSI

Identidad

Servicios de confianza (que incluye firma electrónica)

Paralelismo





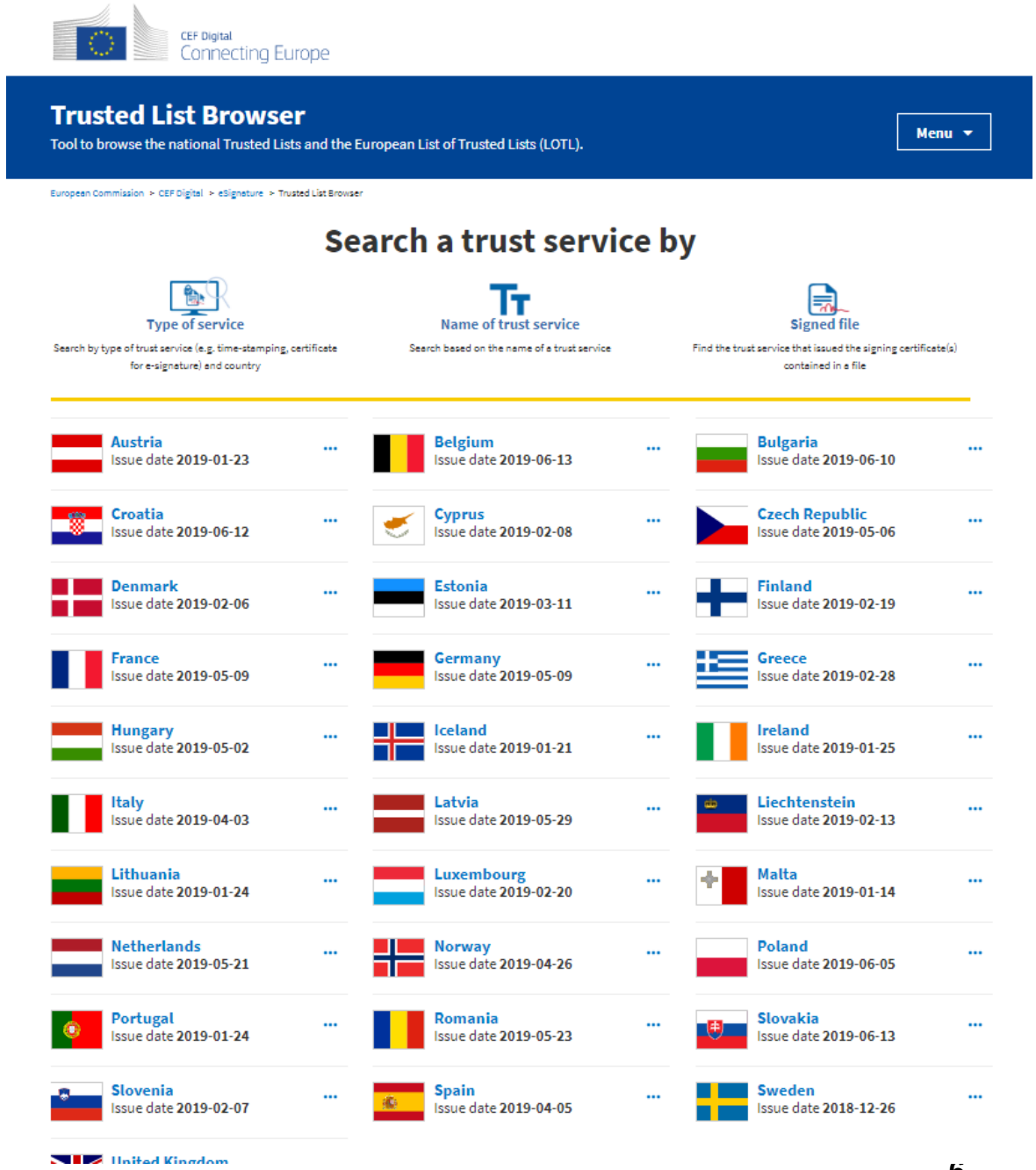
Firma

Firma - Confianza

PSC: Prestador de Servicio de Certificación

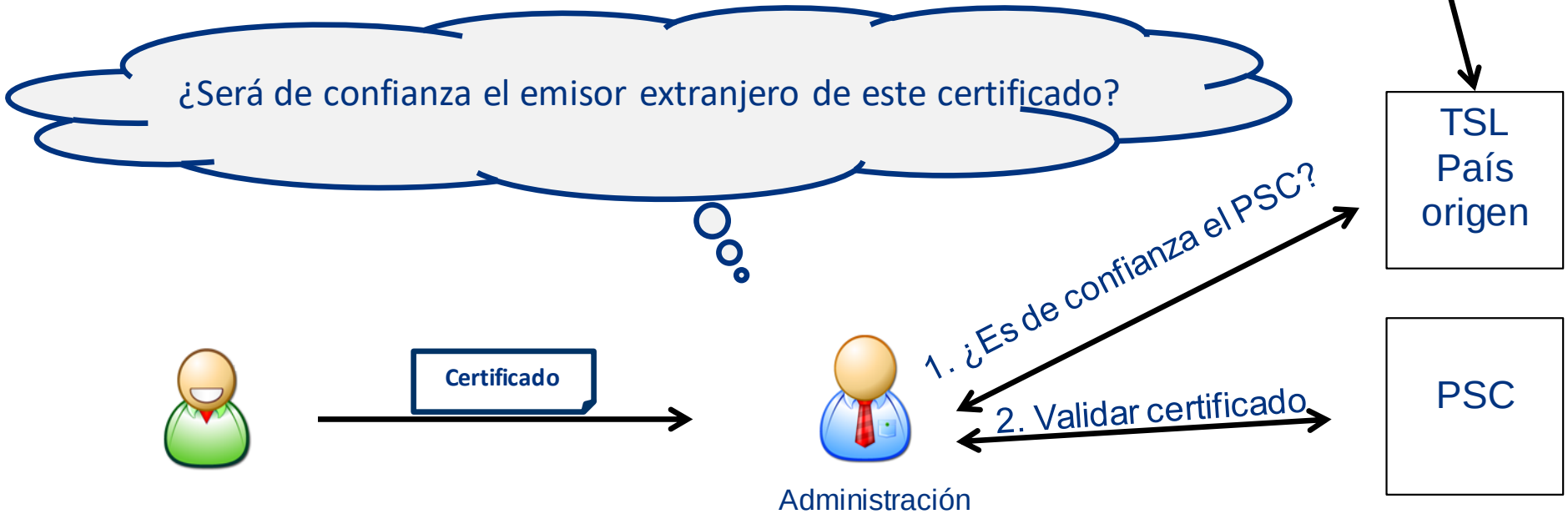
TSL: Trust Service List

- Decisión de Ejecución UE 2015/1505.

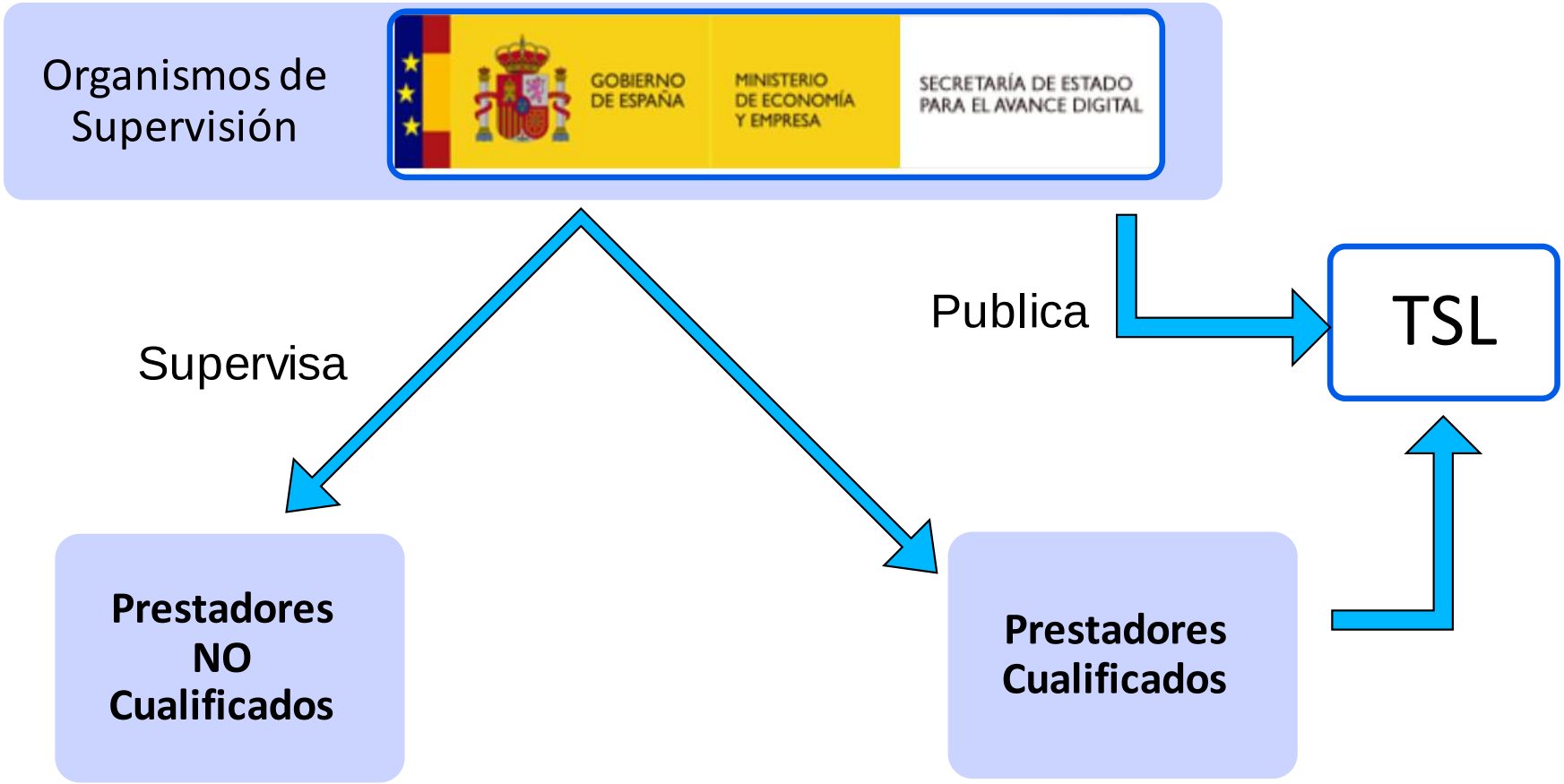


TSL

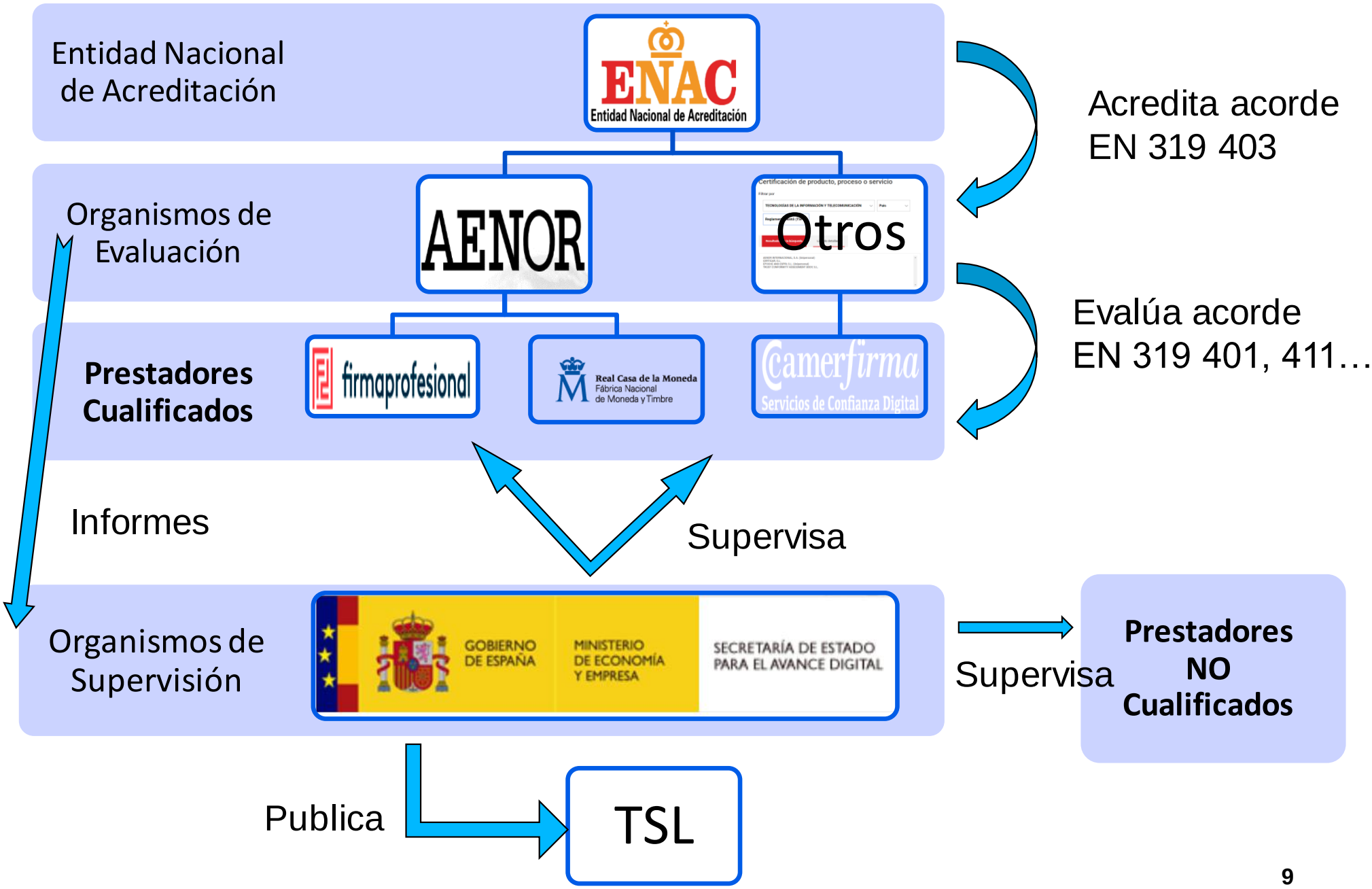

```
            <Name xml:lang="en">Dirección General de la Policía</Name>
            <Name xml:lang="es">Dirección General de la Policía</Name>
          </TSPName>
        + <TSPTradeName>
        + <TSPAddress>
        - <TSPInformationURI>
            <URI xml:lang="en">http://www.dnielectronico.es/PDFs/practice_statement_certification_policy.pdf</URI>
            <URI xml:lang="es">http://www.dnielectronico.es</URI>
          </TSPInformationURI>
        </TSPInformation>
      - <TSPServices>
        - <TSPService>
          - <ServiceInformation>
              <ServiceTypeIdentifier>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</ServiceTypeIdentifier>
            - <ServiceName>
                <Name xml:lang="en">Qualified Certificates issued by subordinated CA under the root CA</Name>
                <Name xml:lang="es">Certificados Reconocidos emitido por CAs subordinadas de la CA Root</Name>
              </ServiceName>
            - <ServiceDigitalIdentity>
              - <DigitalId>
                  <X509Certificate>MIIFvzCCA6egAwIBAgIQANKFcP2up9ZfEYQVxjG1yzANBgkqhkiG9w0BAQUFADBdMQswCQYDVQQGEwJFUzEoMCYGA1UECgwfRElSR
                </DigitalId>
              - <DigitalId>
                  <X509Certificate>MIIFvzCCA6egAwIBAgIQAMUmyW4QlO1DT/e1+2eflDANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJFUzEoMCYGA1UECgwfRElS
                </DigitalId>
              - <DigitalId>
                  <X509SubjectName>CN=AC RAIZ DNIE,OU=DNIE,O=DIRECCION GENERAL DE LA POLICIA,C=ES</X509SubjectName>
                </DigitalId>
              </ServiceDigitalIdentity>
              <ServiceStatus>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</ServiceStatus>
              <StatusStartingTime>2016-06-30T22:00:00Z</StatusStartingTime>
            - <SchemeServiceDefinitionURI>
                <URI xml:lang="en">https://www.dnielectronico.es/ZIP/ACDNIE001-SHA1.crt</URI>
```

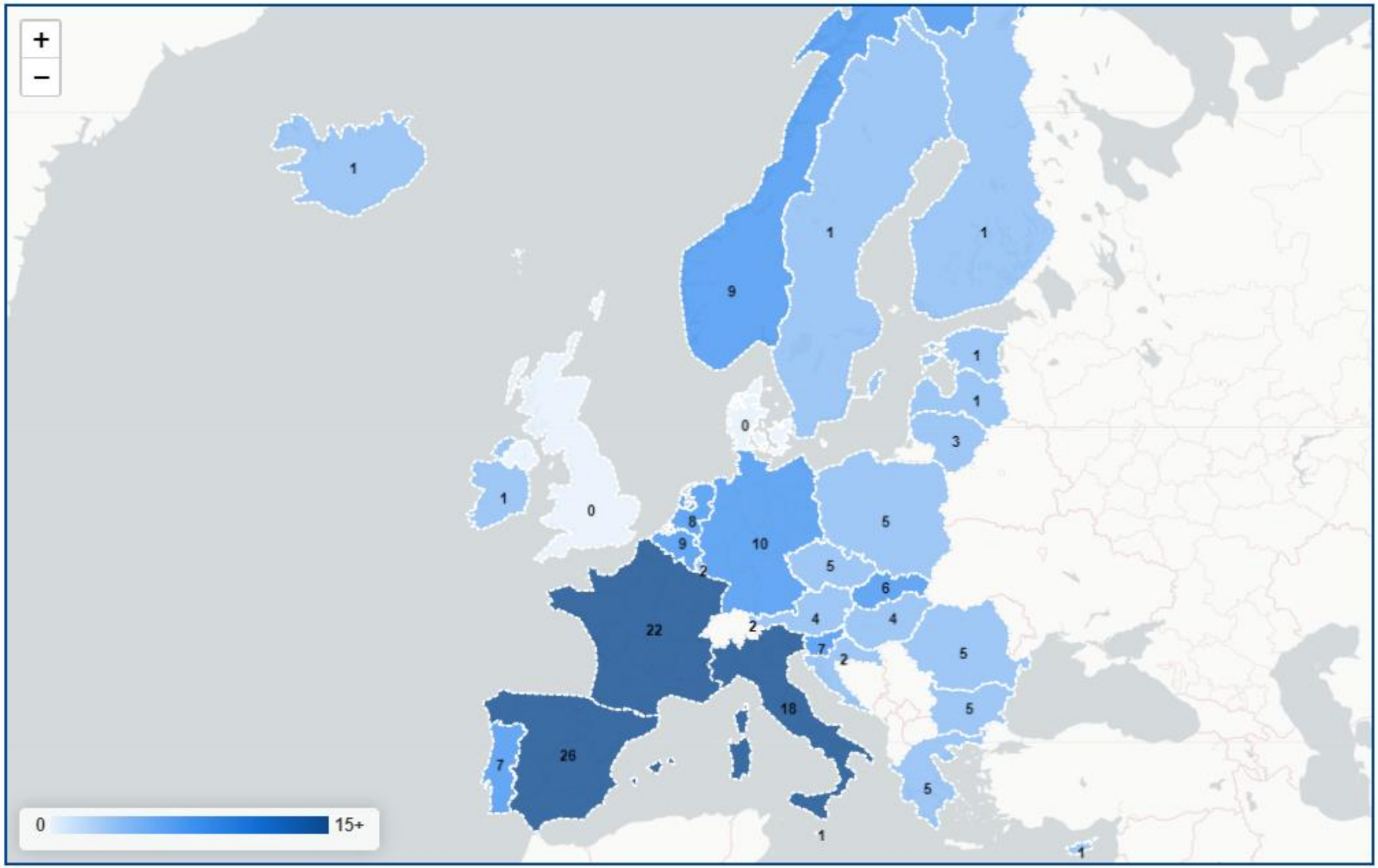



Firma – PSC cualificados



Firma – PSC cualificados

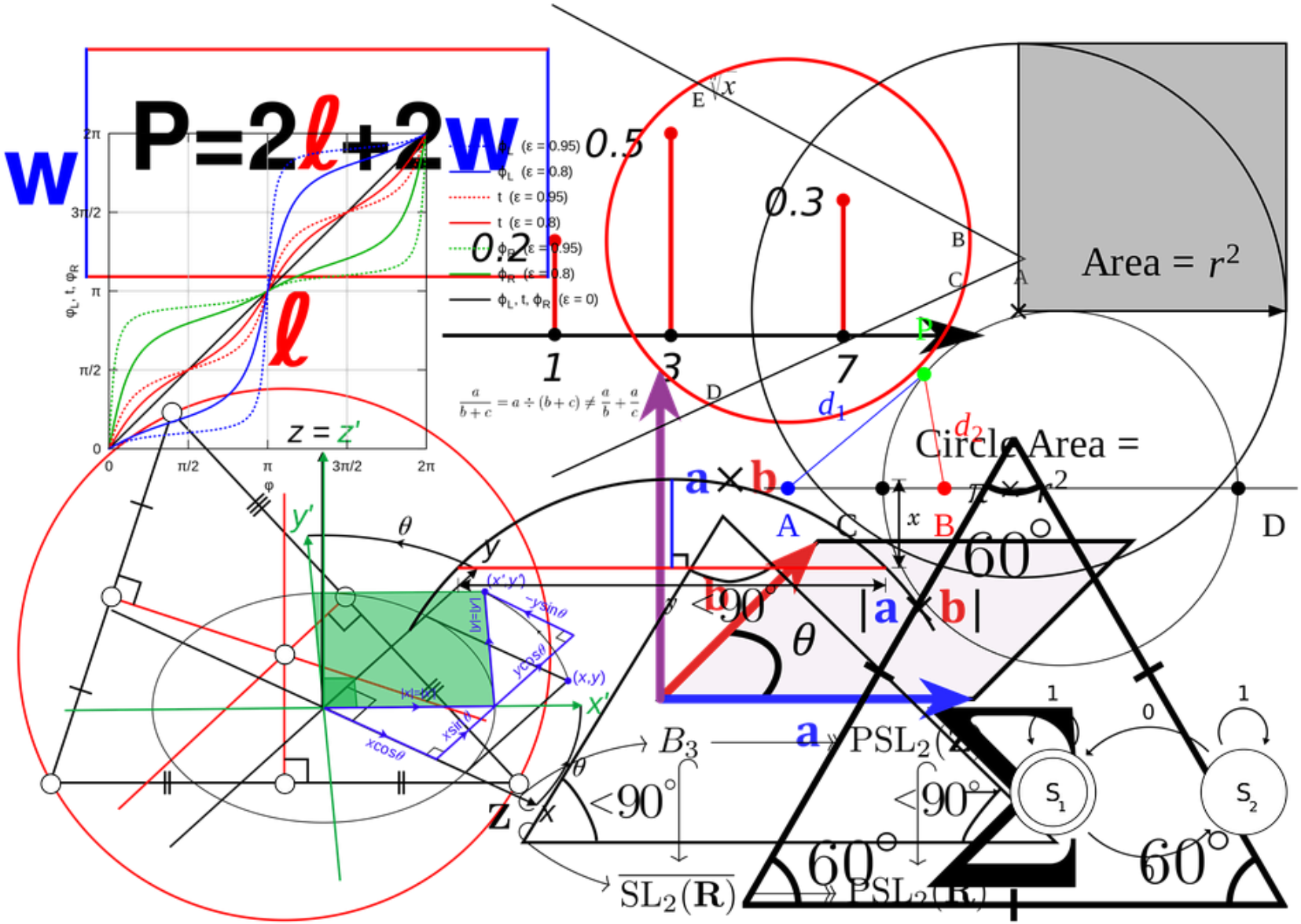



+
−
1
1
1
9
1
1
3
0
1
0
8
9
10
5
2
5
6
22
2
4
4
7
2
5
18
5
26
7
5
1
1
0
15+

Firma- personas jurídicas

- Certificado de **sello** electrónico de Persona Jurídica.
- Certificado de **firma** de Persona Física **Representante** de Persona Jurídica.

- **Decisión de Ejecución UE 2015/1506.**



- Identidad del certificado.
- Seudónimo.

Firma en la nube

- Firma como servicio


FIRma Electrónica - FIRe
Firma solicitada por Aplicación de Pruebas
Cancelar
Seleccione el sistema de firma
cl@ve firma
Firma con Cl@ve Firma
Utilice un certificado de firma de Cl@ve o realice su solicitud si no dispone de él.
Acceder
autofirma
Firma con certificado local
Utilice un certificado instalado en el almacén de claves de su navegador o alojado en tarjeta inteligente.
Acceder
FIRe
© Gobierno de España · FIRe

Interoperabilidad con Europa

Firma realizada con certificado emitido por un PSC de fuera de la UE.

- De momento no tiene base jurídica.
- Articulo 14 del eIDAS

Reconocido en base a acuerdo país-UE.

- Reconocimiento reciproco
- El PSC cumple los requisitos de PSC cualificado.

CONCLUSIONES PARA LA FIRMA

Interoperabilidad:

Organizativa:

- Organismo Supervisor: Supervisión y cualificación de los PSC.
- Esquema común de evaluación de PSC para que sean comparables. (Normas ETSI EN).

Semántica:

- TSL
- Personas jurídicas. (Sellos electrónicos)

Técnica.

- Formatos de firma

Soluciones disponibles:

Suite @firma.

Generador de TSL

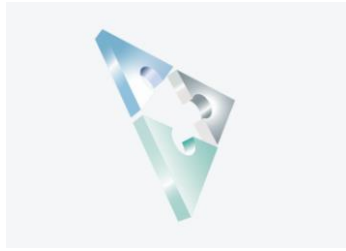
Elementos disponibles

suite @firma

Creación firma | Validación

Cliente: Fire | En servidor: Integr@ | @firma | Integr@

FIRe integra @firma integra

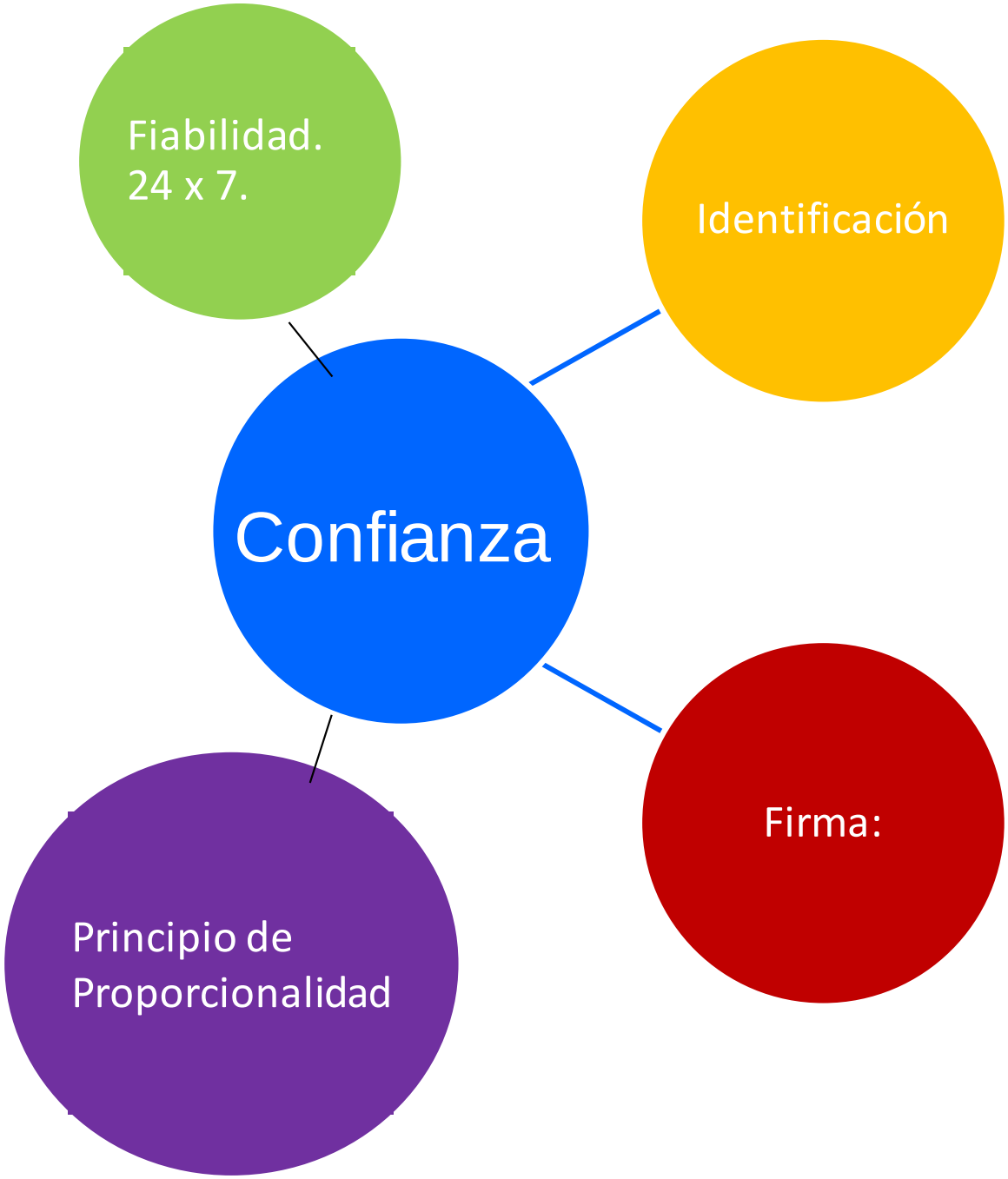


Factores de éxito

Factores de éxito

- Confianza
- Usabilidad
- Armonización
- Modelo de negocio
- Neutralidad Tecnológica
- Marco legal claro y homogéneo

Confianza



- Es clave el registro seguro de los usuarios al sistema.
- Se plantean escenarios de confianza creciente.
- Es clave la supervisión de los prestadores PSC.
- Si esta basada en certificados cualificados, permite el intercambio trasfronterizo.
- La identificación del poseedor de la firma para la expedición y reexpedición de credenciales de firma (presencial cada x años)

Usabilidad

- Identificación:
  - Los medios a los que el ciudadano esta acostumbrado. Password (y segundo factor como SMS al móvil o tarjeta de barcos, etc.). Dejar al ciudadano elegir.
  - Capilaridad para registro en el sistema, o cambiar parámetros relevantes (como el numero de móvil) sin necesidad de firma electrónica.
- En firma:
  - La usabilidad frente a la seguridad: certificados en tarjeta, frente certificados en SW o certificados en la nube.

Armonización

- Colaboración entre países.
- Organismo Impulsor.
  - Agencia o servicio en cada país responsable del impulso y coordinación con el resto de países.
  - Responsable de la supervisión de PSC cualificados.
  - Responsable de los nodos de interoperabilidad de identificación.

Modelo de negocio sostenible

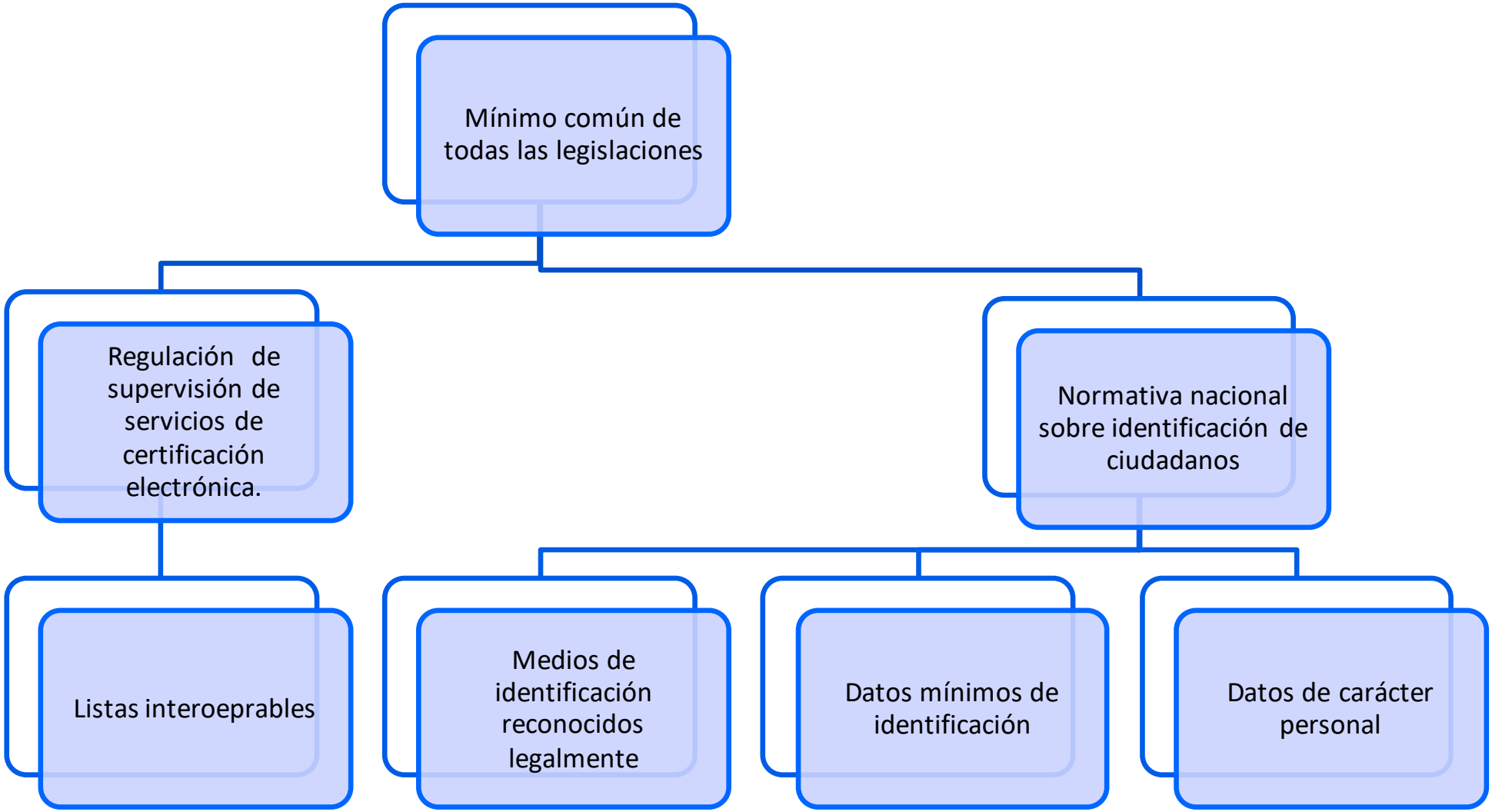
Neutralidad tecnológica

- Enfoque basado en resultados y no en tecnologías
  - Grado de confianza en la autenticidad de la identidad.
  - Confianza en la firma en base a criterios homogéneos de acreditación de PSC.

- Importancia de los estándares
  - ISO / IEC 29115:2013 Marco para el aseguramiento de la autenticación
  - EN 319 403 Trust Service Provider Conformity Assesment. + ISO/IEC 17065)
  - Normas ETSI
  - Federación de identidades: SAML 2.0, OpenID, Oauth
  - …

Marco legal

O acuerdo vinculante común



Muchas gracias