Implementation of Universal Global Trusted Service Provider Identity (Trusted SPID)

Tony Rutkowski
mailto:trutkowski@verisign.com
Co-editor, ITU-T Rec X.idmreq
ITU HLEG member

Trusted-SPID is like doing a “fingerprint” check on the identity of a Service Provider

Service Provider = everyone except end users

Why?

- Historically, the Service Provider trust that is essential for network security was provided by
  - closed, fixed networks
  - operating under substantial domestic and international regulatory regimes
- During the past decade
  - open public networks (e.g., Internet), wireless, globalization, smart terminal devices, application providers, and a shift away from legacy regulatory regimes occurred rapidly
  - without the development of any kind of underlying global service provider trust infrastructure
- The lack of a Service Provider trust infrastructure
  - has contributed significantly to the operations, settlements, security and infrastructure protection problems that adversely affect consumers, providers, and government
  - the abuses will likely continue to increase exponentially without effective Service Provider identity trust remedies

Provider Use Cases

Signalling security	T-SPID is used among providers to control access to signalling and OA&M resources
Traffic exchange and settlements (eliminating Phantom Traffic)	T-SPID is used among providers to manage traffic peering and termination security and settlements
Roaming settlements	T-SPID is facilitate roaming setup and settlements
Content IPR protection; control and fee settlement	T-SPID is used to enable content provider so protect and collect for their IPTV and music programmes
Access of content / application providers to traffic termination providers	T-SPID is used to facilitate access of content and application providers to transport termination capabilities
Threat management; incident response trust capabilities	T-SPID is used to defend against network attacks; do tracebacks; participate in CERTs
Federation interoperability; provider bridging capabilities	T-SPID is used to facilitate federation use and interoperation; provider bridging

Consumer Use Cases

Access trust	T-SPID enables nomadic end user to know the identity and trust of a local access Service Provider
Transaction trust	T-SPID enables an end user to know the identity and trust of a transaction Service Provider
Protection against identity theft	T-SPID enables an end user to know the identity and trust Service Provider to evaluate potential identity theft
Protection of Personally Identifiable Information	T-SPID enables an end user to know the support levels for PPII (i.e., privacy) offered by the Service Provider
Disability assistance	T-SPID enables an end user to know the level of disability assistance supported by the Service Provider
Preventing unwanted intrusions	T-SPID enables SPAM/SPIT reduction
Universal Caller / Sender ID	T-SPID enables the ability of end users to access accurate identity information of callers; call harassment and stalking

Government Use Cases

Government networks	T-SPID is used by agencies to constitute their own global networks
Critical infrastructure protection	T-SPID is used to protect critical national communications and SCADA infrastructure
Emergency telecommunication services	T-SPID is used to enable ETS during disasters
Law enforcement forensics	T-SPID is used to enable the production of criminal evidence
Public safety services	T-SPID is used to enable users to reach emergency call centers or government to send emergency alerts
Universal Service contributions	T-SPID is used to facilitate collection of Universal Service contributions
Number resource allocations	T-SPID is used to manage allocation of telephone numbers, IP addresses, Signalling Point Codes, etc
Network Neutrality	T-SPID is used to enable fair, protected use of transport services

What is required?

- A universal global ability to achieve some trust level in a Service Provider's identity in today's complex network and service environment
  - essential to achieve increased cybersecurity
  - constitutes a special Identity Management implementation known as Trusted Service Provider Identity (SPID)
- Trusted SPID necessitates
  - a universally recognized, globally unique identifier (a kind of call-sign) for each provider
  - combined with the ability to allow instant interoperable discovery and lookup of identity trust resources associated with the provider
- Trusted SPID enables other providers and users to make trust decisions when relying on a provider's identity and assertions in any context or situation
- Governmental and Intergovernmental action
  - Historically a basic role of the ITU
  - Unlikely to occur without governmental support

How?

- Trusted SPID implementations must be
  - decentralized, and sufficiently flexible and technology neutral
    - to accommodate different network, application, provider and user contexts
    - to meet diverse provisioning environments worldwide
    - to avoid adverse effects on innovation or competition
- Although many different legacy and specialized service provider identifiers and platforms exist today, none meet these requirements
  - Specialized to particular uses and individual national agencies or industries, and not universal
  - Not interoperable
  - Not extensible
  - Not available for on-line queries
- Implementation of a Trusted SPID platform seems essential to meet the requirements
  - Before SG17 via Q.6 and Q.10 at the current meeting

Trusted SPID Components

Operations

Unique SPID Identifier Assignment
+
Trust Information Submission

Rapid Resolution of Unique SPID Identifier to Trust Information

Slow Search for SPID Identifier

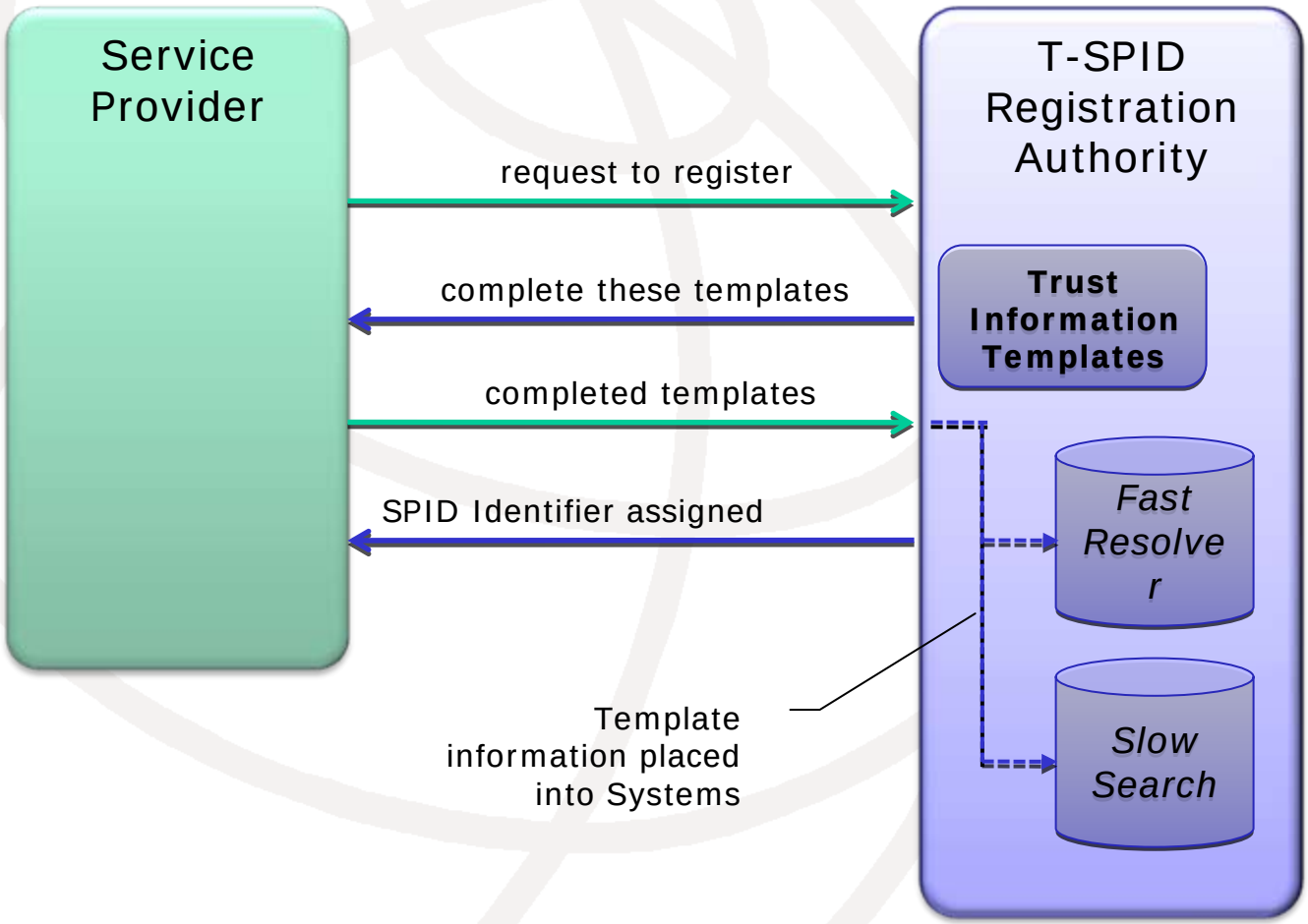
Publication

Publication of Trust Information Templates

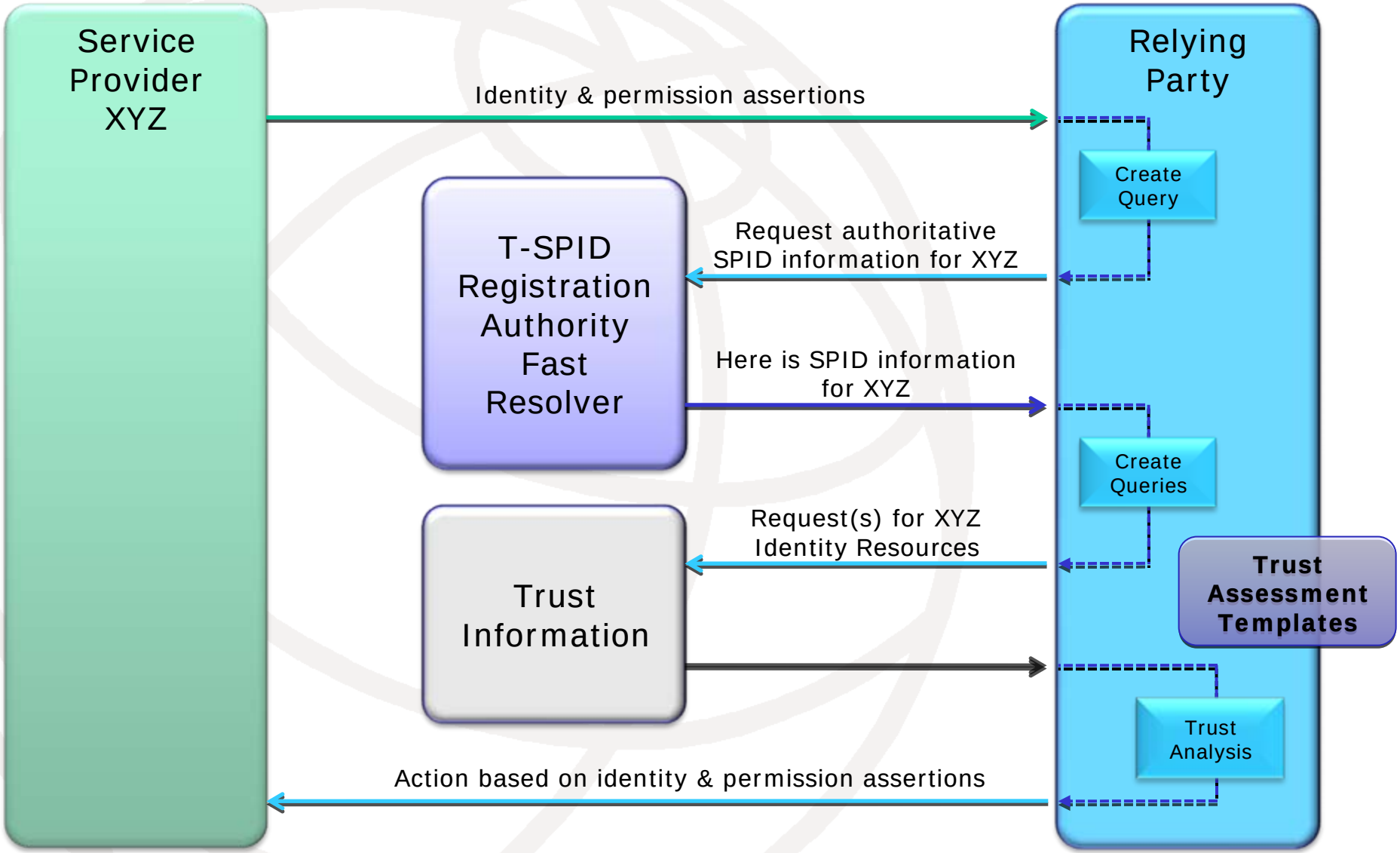
Publication of Trust Assessment Templates

Trust Information

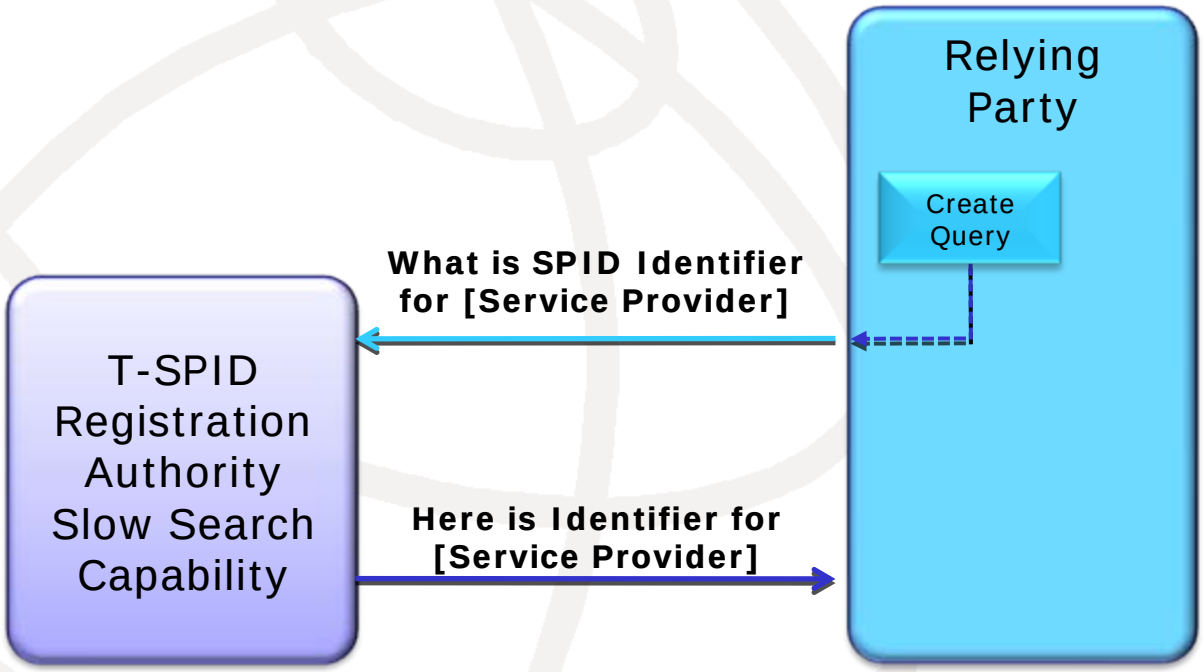
Trusted SPID Registration



Trusted SPID Use
(When the SPID Identifier is known)



Trusted SPID Identifier Search
(When the SPID Identifier is not known)



Leverage what exists

- Trusted SPID requirements can be readily implemented on many different platforms
- A reliable public infrastructure requires robust platforms
- An ideal candidate is found in the past seven years of work on ENUM and ONS
  - ENUM provides service information associated with E.164 number
  - ONS provides identity of an object associated with an EPCglobal Universal Product Code
- Platform can be configured for protected universal open use and performance capabilities
- All of the standards can easily adapted and used by ITU-T
- All of the “running code” can be easily adapted by implementers
- Everything is open source with no intellectual property constraints
- Incents an existing developer community to produce new SPID “trust applications”

Potential Implementations
(Reference Doc. C-286)