

Trusted Service Provider Identity (SPID)

*Technical & Operational Frequently Asked Questions including Use Cases**

What exactly does Service Provider Identity (SPID) do?

SPID is a form of coherent, global “Provider ID” applied to any entity offering electronic communication network services – that enables Relying Parties (i.e., other providers and users) to establish trust (assurance) levels for the provider’s identity and related assertions in order to conduct some activity between the Service Provider and the Relying Party. SPID does NOT ensure trust levels; it only facilitates rapid discovery of available, structured, trust resources pertaining to the Service Provider through global registration and query-response processes with high trust levels.

How does SPID accomplish this?

SPID accomplishes this by getting service providers registered with SPID Registration Authorities (SRAs) around the world who assign unique SPID Identifiers which are then used to discover locations providing third party “trust resources” furnished by the providers. This is done using a special implementation of the Internet’s Domain Name System (DNS). Similar implementations are already deployed for telephone number and electronic product code pointers. The only significant difference is the application of this technology to Identity Management of service providers.

How would this SPID capability generally work, step by step?

Registration steps:

- 1) Service Provider contacts appropriate SPID Registration Authority
- 2) Registration Authority assigns a SPID Identifier consisting of the Registration Authority’s own SPID 3-digit Identifier plus a unique 9-digit number and an optional 3-digit subsidiary number.
- 3) Registration Authority obtains from the Service Provider an array of Trust Resource reference information including the network addresses for that information in special Trust Resource Service templates. One of these templates would generally include digital certificate.
- 4) Registration Authority places this submitted information into an ultra-fast DNS-like system called the SPID Name System (SNS), plus some basic information into a slow registry information system (SREG) that supports distributed searches, security, and auditing capabilities.

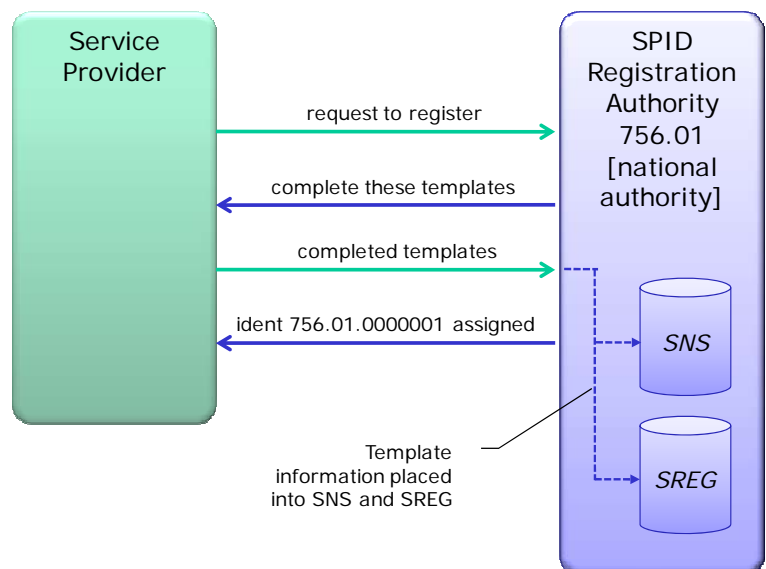


Figure 1 SPID Registration

* A.M.Rutkowski, co-editor, ITU-T Rec. X.idmreq, **Requirements for Global Identity Management Interoperability and Trust.**

Discovery query steps:

- 1) For any transaction with a relying party, a Service Provider conveys its SPID Identifier with that party – together with a digital certificate – in response to a request that is part of some transaction. Optionally, the Relying Party may independently discover this information and begin with the next step.

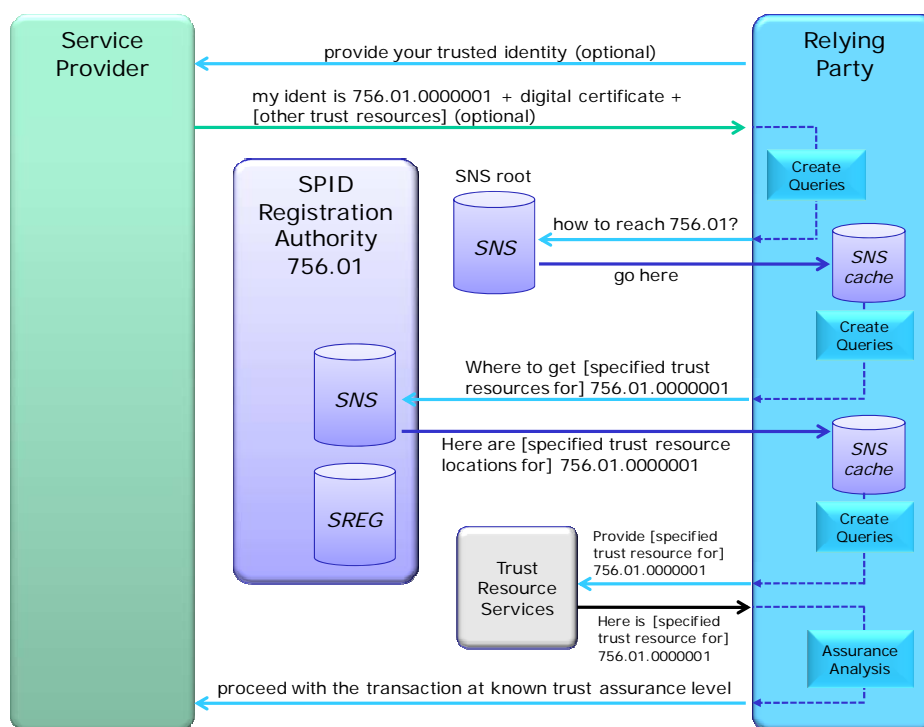
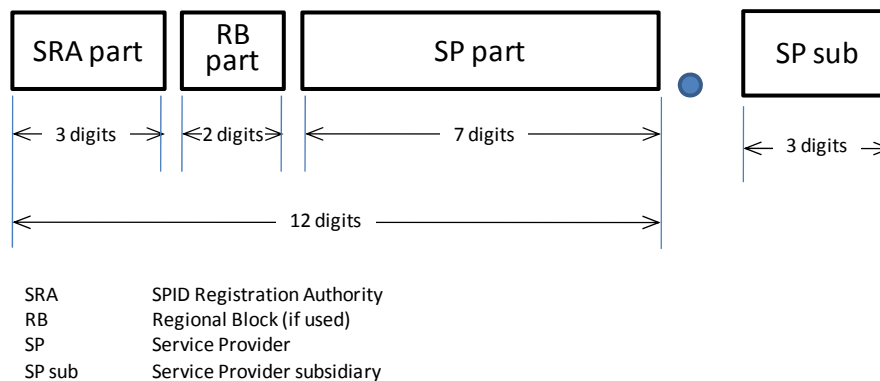


Figure 2 Trust Resource Query (one of many possible)

- 2) Knowing the Service Provider's Identifier, the Relying Party proceeds to find the network address for the SPID Registration Authority (SRA) by a query to the SNS root – which is then locally cached for a specified Time-To-Live by the Relying Party. Generally this is a long time for the root and SRAs.
- 3) The Relying Party then creates one or more queries to the SRA's SNS using for the Service Provider's SPID Identifier. The SRA returns available third party trust resource information (generally in the form of a network address for obtaining the resources) to the Relying Party which caches these results. Some information may be furnished by the SRA itself – especially if it is a government agency and has created the Trust Resource. This information also has a "Time-To-Live" set by the Service Provider or SRA.
- 4) On the basis of those returned results, the Relying Party makes use of the information, generally creating multiple queries to the Trust Resource Service locations, obtaining the relevant information for Assurance Analysis in proceeding with a transaction. The Service Provider's public encrypted PKI or other certificate credentials are usually included.
- 5) Assurance Analysis is generally an automatic program that provides the Relying Party with a level of trust in the Service Provider's identity, assertions, and services in the context of the specific transaction. The Assurance Analysis programs use templates that can be distributed or obtained from a common trusted source.
- 6) There are many possible variations to the above query-response processes, to reflect a great array of different use cases. Indeed, the open standards and the programmable pointer query capabilities (NAPTR) to trust resources using structured, extensible service profiles, allows for an entirely new "trust operating system" on which innovators can build new Identity Management capabilities.

How was the SPID Identifier created?

The SPID Identifier parameters were chosen to optimize both flexibility and extremely high performance on a DNS infrastructure, as well as remain reasonably short for use in protocol “handshake” header fields, yet large enough to accommodate every likely registration authority and provider deployment that could emerge worldwide for the foreseeable future, including its subsidiaries. The identifier consists of the following parts.



The SRA part allows for nearly 1000 Registration Authorities to be established. Today, the ISO has assigned 246 of the SRA numbers to countries or territories, so about ¼ of the codes are available for transnational Registrar use. Allowance is made for the potential division of national registration authorities into regions, provider types, or competition arrangements through the use of a Regional Block part. The SP part allows up to 10 million providers within each of 99 RP part within each SRA part for a maximum of one billion providers per SRA. Allowing for up to nearly a 1000 subsidiaries per provider should accommodate any potential provider organization substructure. Lastly, the use of all “9”s is reserved as a potential extensibility mechanism for alternative number sets.

Why should this Trusted SPID implementation be trusted? How vulnerable is this system itself?

Trust is always relative. However, systems can be designed to maximize the baseline trust and provide for incremental additional levels of trust. The SPID Name System (SNS) technical platform is the DNS protocol which has existed for many years as a globally-distributed, core, trusted name resolution platform that operates at extremely high performance and reliability levels with widespread caching to improve availability. SNS is expected to be deployed as a protected “infrastructure” among providers with public mirrors available to external users. The vulnerabilities and attacks possible for DNS platforms are well understood and manageable. The vulnerabilities of encrypted digital certificates and their use are well understood and manageable.

SPID Registration Authorities that support the SNS are themselves registered with the root registrar under joint management by the International Telecommunication Union and the Organization for Standardization – and established through cooperation between government authorities and industry. Individual national implementations can implement additional security and trust features.

SRA and Trust Resource Service trust should be essentially self-regulating, as any significant continuing compromise in their trust levels will result in Relying Party users depreciating their trust value through the exchange of trust assurance profiles - much like national registries for ships at sea. Conversely, trust and security equates with improved eCommerce – which also motivates “best of breed” behavior.

What kinds of trust resources can be provided?

DNS specifications are very flexible in providing available information. In particular, the NAPTR pointer mechanism to any published trust resource service that is described for SPID combines a “regular expression (REGEX)” format and optional discovery fields that make this platform not only fast, but almost infinitely flexible. Any kind of provider trust resource - including existing legacy identifiers - for which some utility exists for someone, can be easily deployed. This mechanism also allows for special access, security, and auditing controls for these trust resources.

Because this is the same mechanism now deployed for ENUM telephone numbers and for EPC product codes, there are ample examples of this kind of dynamic deployment, as well as lots of “running code” and templates. Some examples of provider trust resources are depicted in the table below, although it is expected that the marketplace combined with the incentives of an open developer platform will drive innovation and deployment of new Trust Resource Services.

| Category | Type and Description |
|-------------|---|
| Credentials | <ul style="list-style-type: none"> • PKI digital certificates, including associated OIDs and life-cycle status mechanisms (e.g., OCSP) • Other forms of digital certificates or credentials provided to or created by the Registration Authority or a third party Trust Resource Service made available through any medium |
| Identifiers | <ul style="list-style-type: none"> • Cross references to SPID Identifiers in other Registration Authorities • Any assigned or allocated network addresses or identifiers (e.g., IP address handles, E.164 number allocation identifiers, M.1400 ICCs) • Government agency identifiers (e.g., tax, regulatory, consumer protection, justice, public safety, homeland security) • Federation identifiers |
| Attributes | <ul style="list-style-type: none"> • Legal name • Incorporation jurisdiction • Services supported, especially mobile services • Geolocation information • Addresses for discovery and queries concerning customer identities, especially for CallerID and directory services • Services supported, especially emergency telecommunication services • Security capabilities supported • Privacy guidelines or requirements supported • Disability assistance capabilities supported • Mechanisms and addresses for settlement of accounts among providers, especially for content distribution |
| Patterns | <ul style="list-style-type: none"> • Structured reputation information |

What kinds of use-cases does Trusted SPID support?

| Category | Type and Description |
|------------|--|
| Providers | <ul style="list-style-type: none"> • Traffic peering security; settlements • Traffic termination security; settlements • Gateway traffic (e.g., SMS, VoIP) security; settlements • Roaming settlements • Enhanced IPR protection; content fee settlements • Enhanced access of content and application providers to traffic termination providers • Improved network security; management; incident response capabilities • Federation interoperability and provider bridging capabilities |
| Consumers | <ul style="list-style-type: none"> • Access security • Transaction security • Identity theft minimization • Enhanced roaming capabilities • Privacy protection enhancements • SPAM & DoNotFax/Call minimization (including VoIP & SMS SPAM) • Universal Caller/Sender ID • Disability assistance enhancements |
| Government | <ul style="list-style-type: none"> • Private network security (e.g., GIG) • Critical infrastructure protection • Enhanced emergency telecom services interoperability and use • Law enforcement investigation support (LI, retained data, and forensics) • Public safety services enhancements (e.g., message alerts) • Universal Service settlements • Number resource management enhancements (telephone numbers, IP addresses) • “Network neutrality” facilitation |

What benefits does Trusted SPID really provide...and is it worth the effort?

Service Provider Identities in various forms have been around since the first interconnection of networks. Trusted identity among providers on a global basis is what made worldwide reliable and secure communication networks possible as everyone shared each other’s resources and worked out the compensation arrangements through the ITU and its precursors. It was a single global federation backed by law.

That legacy architecture began to end with a combination of wireless nomadic users using their own smart terminal devices, with open IP-enabled networks, with common carrier deregulation, and with new breeds of ICT providers plugging their service facilities into the emerging global public network infrastructure. Trusted identity among providers has disappeared except in small disaggregated federations of providers. The resulting chaos over the past ten years has resulted in the exponential disappearance of reliable and secure global networks and services with no end in sight.

Everyone – providers, consumers, and governments - can continue to cope with the chaos in their own way and hope for the best. Or they can collectively begin doing something about it.

The ITU as well as almost every government agency in every country and lots of private-sector companies and organizations maintain many different species of legacy and specialized SPIDs for all

kinds of specific purposes today. However, they all exist in their own compartmentalized sectors of contractual agreements and federations, and none are capable of globally enabling trust levels among all network constituents.

Trusted SPID is not a cure-all for everything involving network/cyber security. It begins with the simple value proposition of 1) a unique identifier for every network/ICT service provider that can be used to rather instantly find out authoritative basic identity information associated with that provider that can be 2) used “on-demand” to immediately establish some desired trust level in using the provider’s service. Use is optional and flexible - rather like checking a provider’s driver’s license or fingerprints with national authorities – depending on the action involved.

Trusted SPID is being architected as a coherent structured global overlay of registries that uniquely identifies every provider and provides instant pointers to their registered digital credentials, existing issued identifiers, attributes, and reputation information. Trusted SPID relies significantly on the three most ubiquitous and effective means for enabling “trust-on-demand” – encrypted PKI certificates, a special “programmable” version of the Domain Name System, and national government backing. It’s not invulnerable, but it is a “best of breed” approach that is capable of continually evolving and scaling.

The alternative is essentially maintaining islands of providers and users and coping with the exponentially growing losses to consumers, providers, and governments measured not only in money, but also in resulting vulnerabilities, including diminished public safety and national security.