

Signature and Proof Infrastructure

OpenTrust SPI

Digital Signature Basics



State of the Art

- Increasing demand for e-business processes and paperless transactions
- Need to increase the level of trust using strong authentication and digital signatures
- Factors inhibiting widespread use of digital signatures:
 - Specific implementation of signature solution for each business application
 - Legal risks and challenges difficult to understand
 - Insufficient signature and proof experience and methodology
 - Signature solutions are often complex to integrate

Regulations and Standards

- Regulation Framework



- European Directive 1999/93/CE, December 1999



- Loi n° 2000-230 Mars 2000, Décret n° 2001-272 Mars 2001



- Electr. Communications Act 2000, Electr. Signatures Regulations 2002



- German Act on Digital Signature 2001, Signature Ordonnance 2001



- US SEAL (1998), UETA (1999), ESIGN (2001)

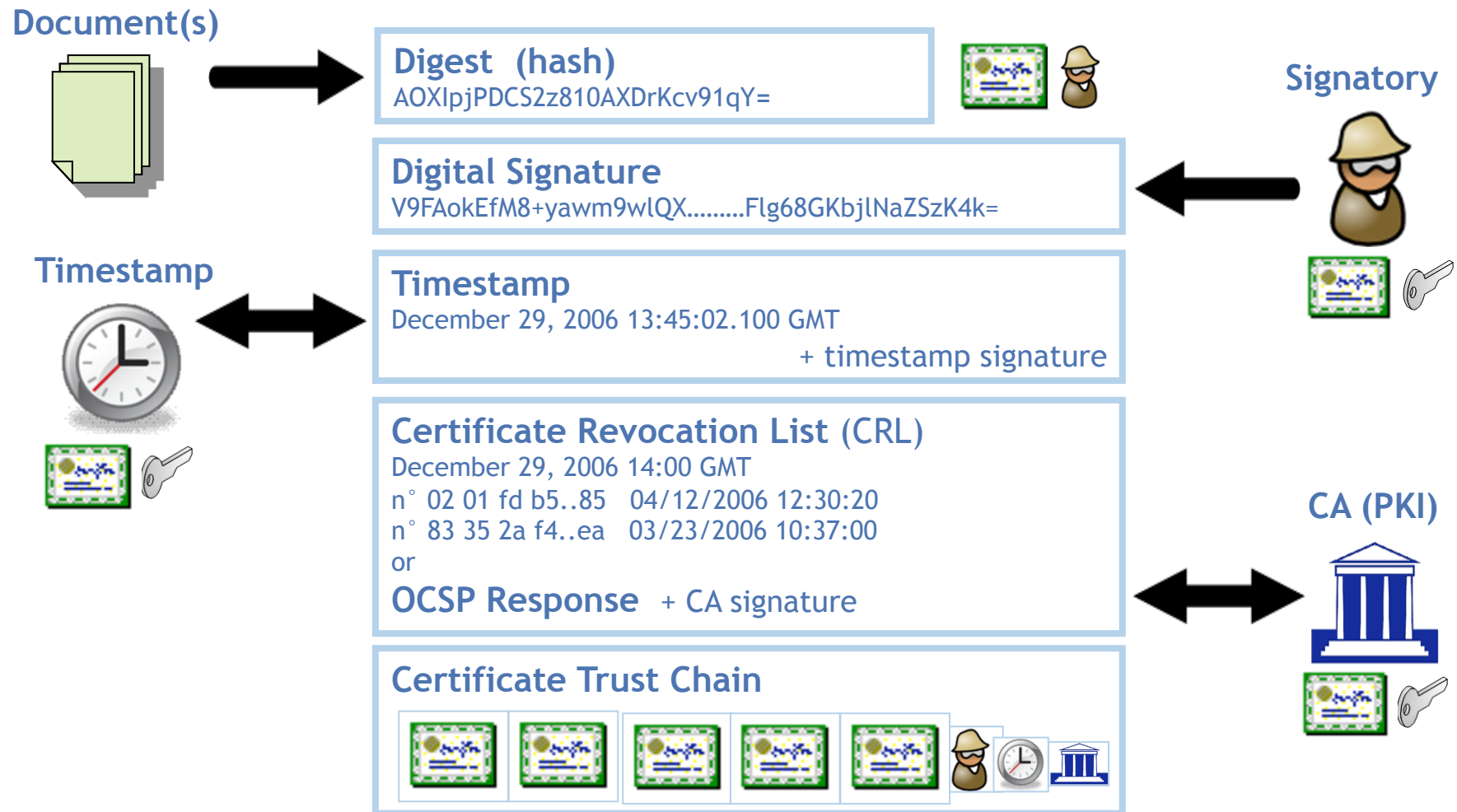
-

- Signature Formats

- ASN.1/DER format: PKCS#7, CMS (RFC 3369), PDF Signature, CADES

- XML format: XML-DSIG, [XADES \(ETSI TS 101 903\)](#)

Digital Signature - Technical Elements



From Digital Signature to Electronic Proof

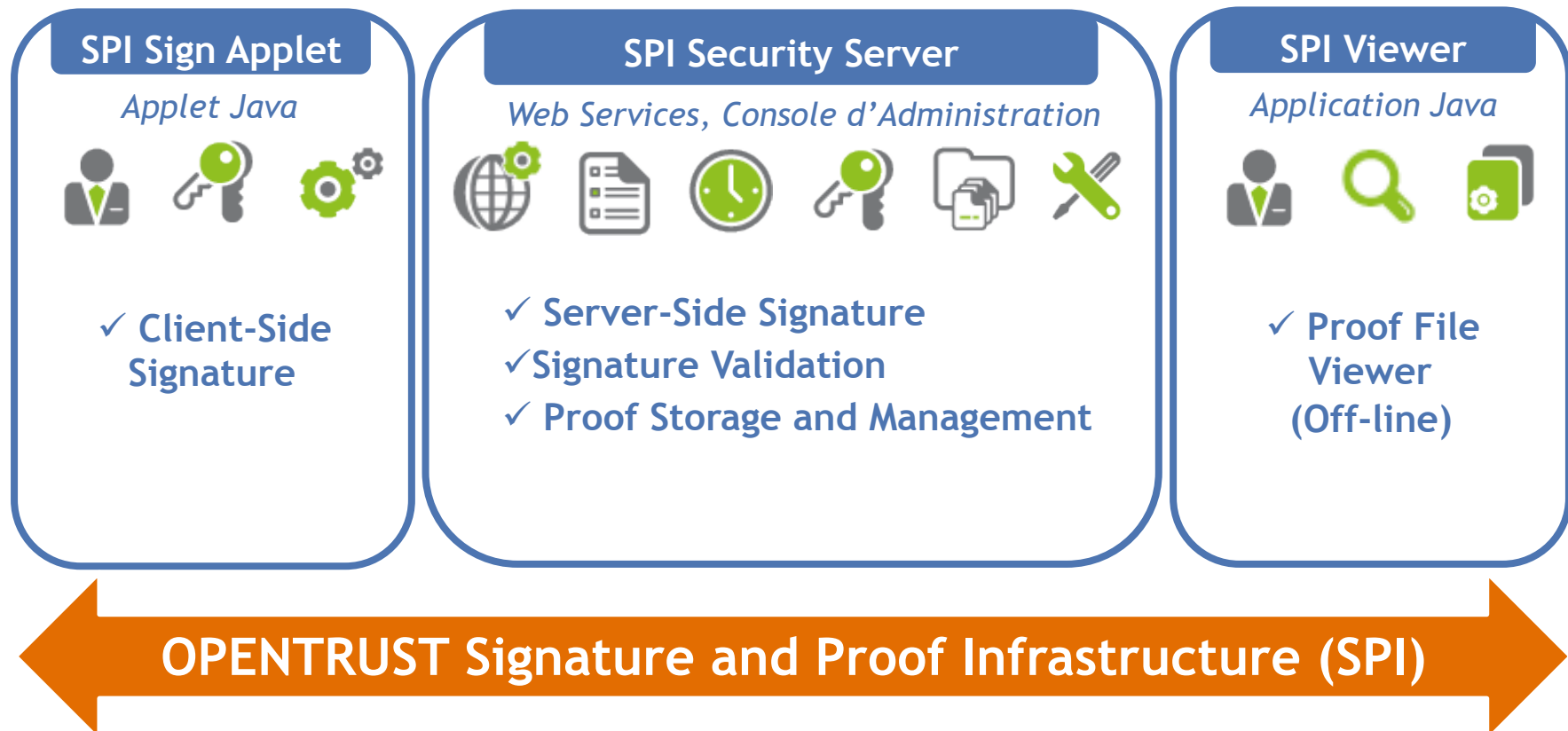
- **Digital Signature**
 - Authentication, integrity and non-repudiation
 - Equivalent to hand-written signature when regulation is followed
- **Electronic Proof**
 - Collection of data and information of probative value
 - Content depends on a proof policy
 - This policy must have been approved and agreed upon by all concerned parties

Signature and Proof Infrastructure OpenTrust SPI

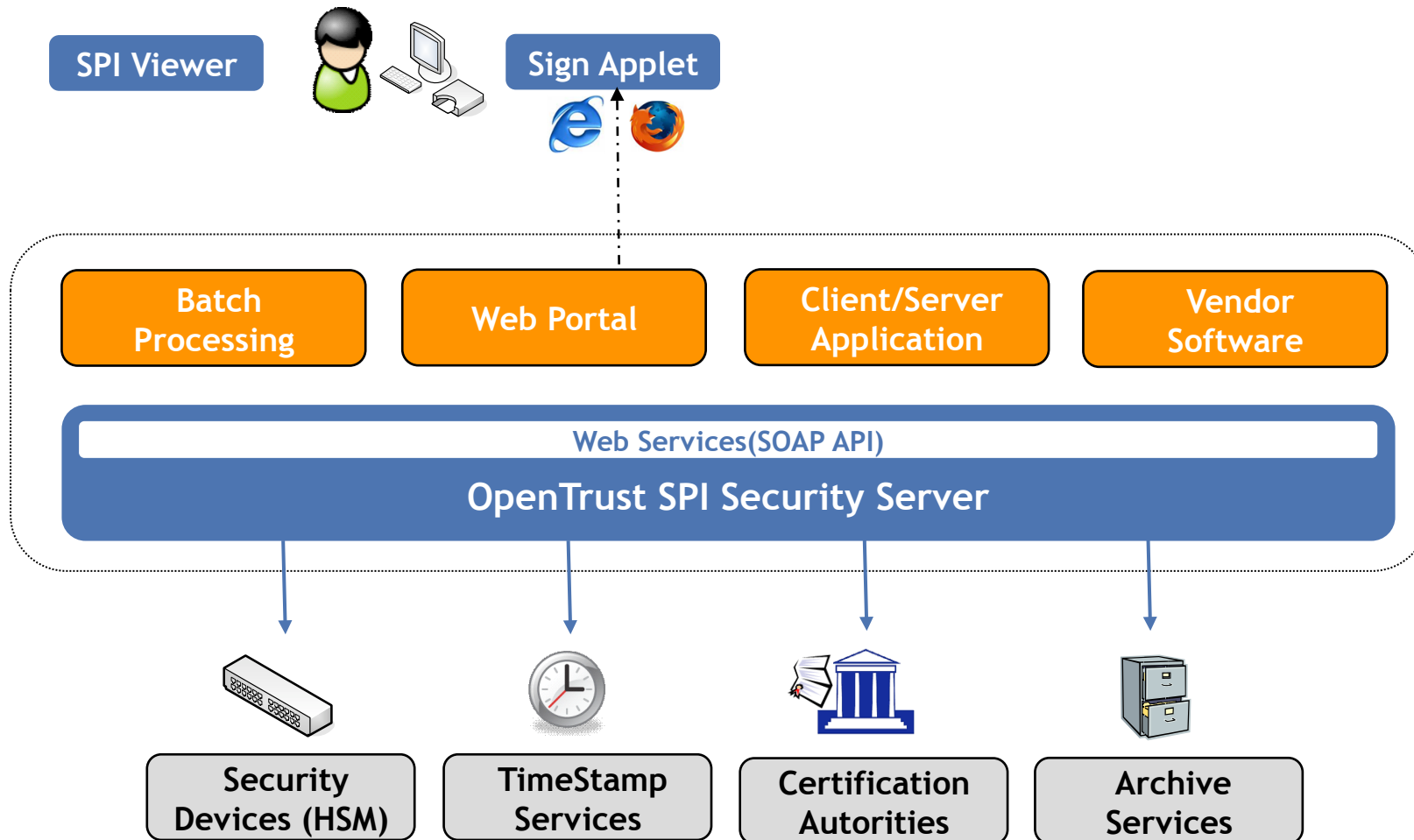
Concepts and Functionality



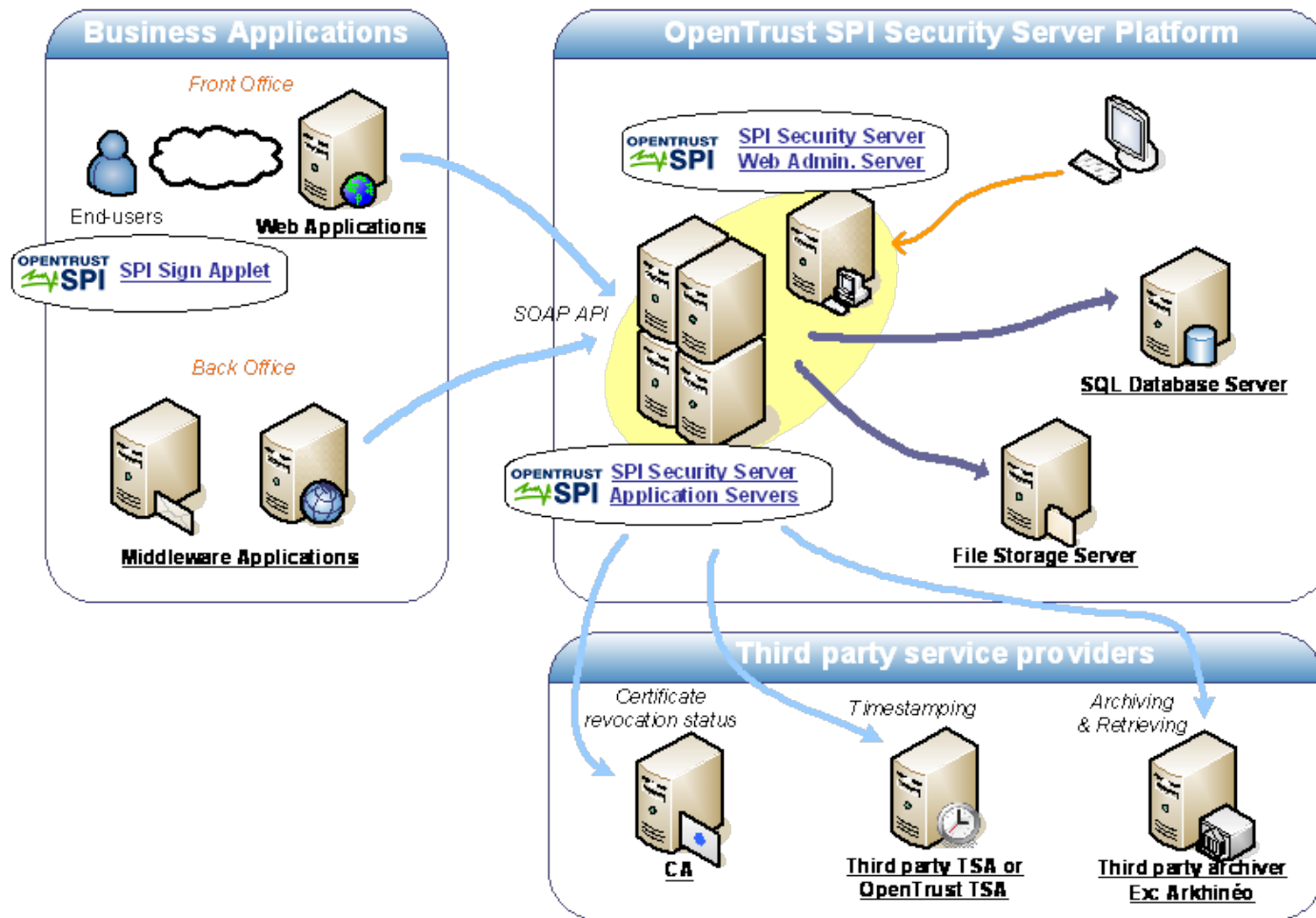
A Complete and Proven Solution



Quick and Straightforward to Integrate



Opentrust SPI Technical Architecture



OpenTrust SPI Security Server Features

- **System Administration and Technical Functions**
 - Management of user and administrator accounts, along with associated rights
 - Management of signers (key pairs for automated server signature)
 - Management of machines (SPI Security Server application instances)
 - Management of logs and audit trails
 - Management of Trusted Certification Authorities
 - Management of platform configuration parameters
- **Profiles and Policies Management Functions**
 - Proof profiles
 - Signature policy and profile
 - Timestamping profile
 - Storage and Archiving profiles
- **Electronic Signatures Web Services**
 - Simple signature and validation services
 - Proof management services

SPI Administrative Console - Log & Audit

The screenshot displays the OPENTRUST SPI Administrative Console interface. The top header features the OPENTRUST logo on the left and the SPI logo on the right, with the user 'admin' logged in. Below the header is a green navigation bar labeled 'System Administration'. A left-hand sidebar contains a menu with items: Accounts, Certificates, Platforms (expanded), Machines, Log & Audit (selected), Configuration, Cache, Jobs, Providers, and Batches. The main content area is titled 'Platforms / Log & Audit' and contains an informational box with the following text: 'Here you may remotely view and manage machines log and browse the platform centralized audit trails. The first two tabs are used for log consultation. Non-audit Logs are written in local files on every machine. Audit trails are written in the centralized database. The last two tabs allow you to modify log configuration: ^ in the database, used by SPI at next startup ^ live modification, lost at shutdown. Error details log files must be fetched directly on the machine (no viewer exists).' Below this box are four tabs: 'Log Viewer', 'Audit Viewer', 'Log Config', and 'Live Log Level'. A 'Log Viewer' window is open, showing a table with two rows: '1 Select Machine' with value 'machine1 | ws' and '2 Select Channel' with value 'OPER PERF TECH APPLI'. The footer of the console includes the OPENTRUST logo and the text 'contact | help | ©_OPENTRUST.2007'.

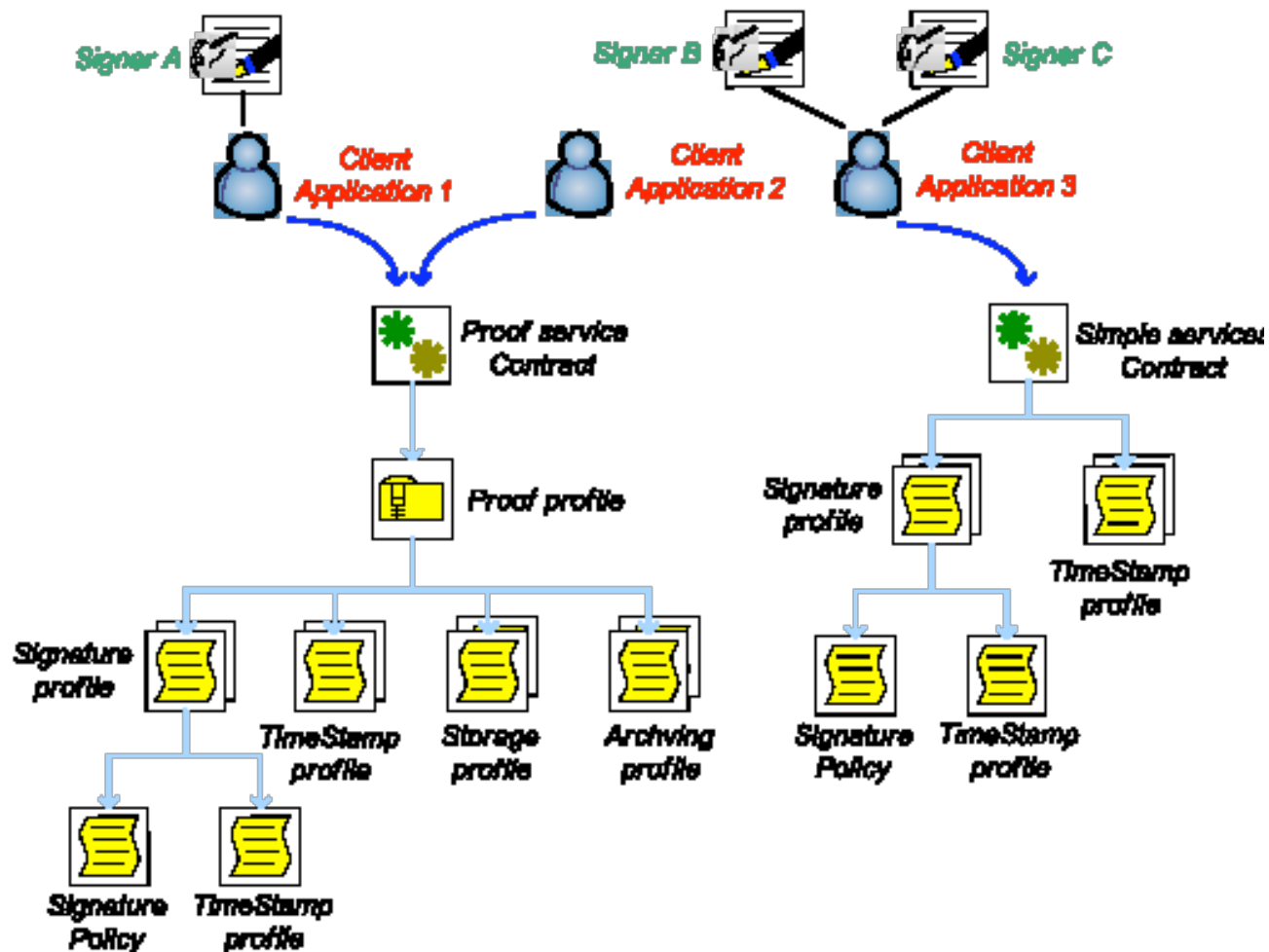
SPI Administrative Console - Profiles Management

The screenshot displays the OPENTRUST SPI Administrative Console interface. At the top, the OPENTRUST logo is on the left, and the SPI logo is on the right. Below the logo, a green bar contains the text "Services Administration" on the left and "admin" on the right. A left-hand navigation menu features three items: "Contracts", "Profiles", and "Records", each with a right-pointing arrow. The main content area is titled "Profiles". Below the title is an information box with a blue 'i' icon and the text: "Here you may manage profile objects used for generating and verifying digital signatures and proof records. Profiles must be referenced in service contracts for a client to be able to use them in requests." Below this is a form with a label "Select profile type" and a dropdown menu currently showing "Signature Policy". To the right of the dropdown is a lightbulb icon. Below the form is a button labeled "Add new profile" with a lightbulb icon. At the bottom of the main content area is a table with the following data:

active	Profile ID	Profile Description	Action
<input checked="" type="checkbox"/>	OT-SPO-DEFAULT	Default signature policy	Edit View
<input checked="" type="checkbox"/>	P-SPO-TESTWEB1	Test profile creation in console	Edit View

At the bottom center of the page, the OPENTRUST logo is displayed above the text "contact | help | © OPENTRUST 2007".

Contracts, Profiles & Policies Design



Summary of OpenTrust SPI

- Respect of standards and regulatory framework
- Support for multiple signature formats

- An integrated middleware platform
- An evolving SOA

- Feature-rich and flexible to use
- Management of object policies and policy models

- Security & performance
- Packaged product and associated services

OpenTrust SPI Security Server Features

- **System Administration and Technical Functions**
 - Management of user and administrator accounts, along with associated rights
 - Management of signers (key pairs for automated server signature)
 - Management of machines (SPI Security Server application instances)
 - Management of logs and audit trails
 - Management of Trusted Certification Authorities
 - Management of platform configuration parameters
- **Profiles and Policies Management Functions**
 - Proof profiles
 - Signature policies and profiles
 - Timestamping profiles
 - Storage and Archiving profiles
- **Digital Signatures Web Services**
 - Multi format signature and validation services
 - Proof management services

Summary of OpenTrust SPI

- Signature standards and regulatory framework conformance
- Support for multiple signature formats
- Feature-rich and flexible to use
- Management of signature profiles and policies
- Security & performance
- Packaged solution and associated professional services

Signature and Proof Infrastructure OpenTrust SPI

Client Cases



Paperless Temping Contracts

Context

- The PIXID portal, created by Adecco, Manpower and VediorBis, provides the temporary employment industry with an e-administration platform enabling:
 - ✓ Control and traceability,
 - ✓ Increased productivity.
- This platform is particularly useful for the signature of temping contracts that must be rapidly signed when a mission begins.

Key Elements

- 200 customer companies connected; 1000 users,
- 35 temporary employment agencies connected,
- 2500 agencies already configured,
- 10 000 tempory employment contracts exchanged each month between customer companies and temping agencies via the e-platform.

Approach and Proposed Solution

- Pixid chose the OPENTRUST SPI solution to ensure the following functions:
 - ✓ Client-side signature (SPI Sign Applet and ActiveX)
 - ✓ Digital proof validation and management (SPI Security Server)
 - ✓ Visualization of proof details (SPI Viewer)

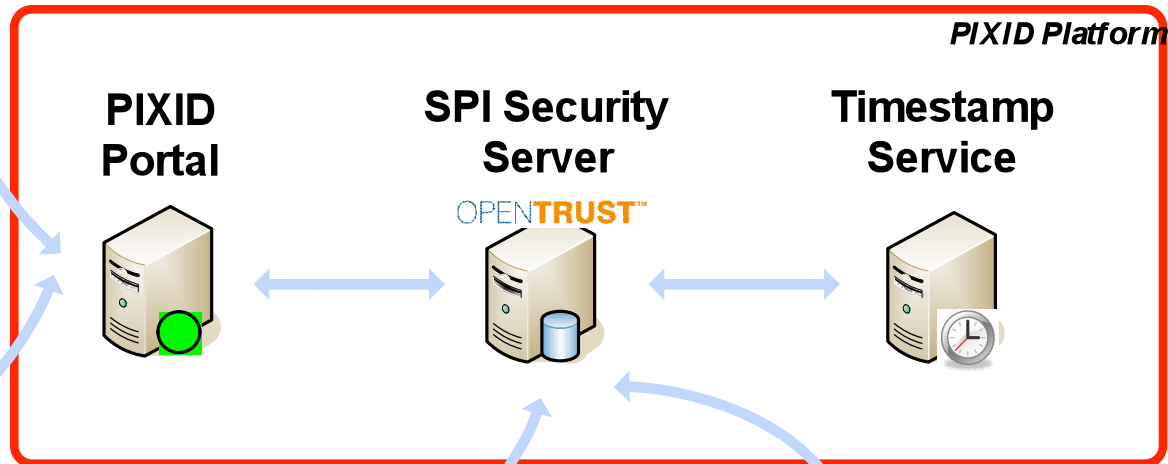
Technical Elements

- Server Environment: Sun Solaris, WebLogic, Oracle, SPI Security Server, Apache OpenTSA, CDC Arkhineo.
- Workstation: Windows, Internet Explorer, Netscape, Mozilla, Firefox.

Temping Agency



Temping Customer



Paperless Supplier Contracts

Context

- Carrefour France wished to set up a secure e-process for rapidly exchanging and signing contracts for promotional operations and services with suppliers. The aim was to:
 - ✓ Simplify and lighten a heavy administrative procedure
 - ✓ Reduce risks of fines stemming from invalid promotions in the absence of a signed contract.
- Contracts established in all formats stipulated in the company charter.

Key Elements

- 85% of Carrefour France's supplier contracts
- Over 80 000 contracts per year
- Over 1 000 signatories (440 food suppliers and 635 non-food suppliers).

Approach and Proposed Solution

- Carrefour chose the OPENTRUST SPI solution for the following functions:
 - ✓ Mass signature for the AdCo buying service (SPI Autosign)
 - ✓ Supplier signatures (Sign Applet)
 - ✓ Validation and management of electronic proof (SPI Security Server)
 - ✓ Visualization of proof details (SPI Viewer)

Technical Elements

- Server environment: Linux, JBoss, Oracle, SPI Security Server, OpenTSA
- Workstation: Windows, Internet Explorer, Netscape, Mozilla, Firefox.

