

Novell's Identity Assurance Solution for HSPD-12

An open, standards-based identity and access management system that validates identities and authenticates users for privileged access to government IT resources and physical facilities.

Position Paper

Novell.

Table of Contents

EXECUTIVE SUMMARY.....	3
HSPD-12 SOLUTION ARCHITECTURE OVERVIEW.....	6
ENROLLMENT & REGISTRATION.....	7
CARD ISSUANCE & MAINTENANCE	8
LOGICAL & PHYSICAL ACCESS CONTROL.....	8
EVENT MONITORING & MANAGEMENT	9
APPENDIX A. NOVELL SOLUTION OVERVIEW.....	10
DESCRIPTION	10
THE ROLE OF IDENTITY MANAGEMENT.....	11
ACRONYMS.....	12
SYSTEM DESCRIPTION IDMS/CMS	12
FUNCTIONAL INTERFACE DESCRIPTION.....	13
REVOCAION USE CASE	15
APPENDIX B. HSPD-12 PROFESSIONAL SERVICES	17
APPENDIX C. ENTERPRISE DEPLOYMENT ARCHITECTURE.....	22
APPENDIX D. IDENTITY ASSURANCE SOLUTION ROADMAP	23

Executive Summary

“The price of freedom is eternal vigilance.”
—Thomas Jefferson

History of HSPD-12

In August 2004, as part of ongoing efforts to heighten resource protection within government agencies, President Bush issued Homeland Security Presidential Directive (HSPD-12). HSPD-12 directed the Secretary of Commerce to establish a policy for a common identification standard for all federal employees and contractors, and to do so within six months. By establishing a standard for secure identification, the intent of the directive is to protect against a wide array of threats, including unauthorized access to government resources, terrorism and identity theft. Implementations based on the standard will grant federal government employees and contractors secure access to both logical systems and physical facilities.

In February 2005, Commerce Secretary Carlos Gutierrez issued the Federal Information Processing Standards Publication, Personal Identity Verification (PIV) for Federal Employees and Contractors (FIPS PUB 201). It is the definitive document for determining the scope and implementation of HSPD-12. The identification standard, as delineated in the FIPS PUB 201 document, addresses operational requirements, technical frameworks, architecture and specifications for an automated system that provides secure and reliable forms of identification.

According to the standard outlined by the FIPS PUB 201 document, a secure and reliable automated system that complies with HSPD-12 must establish the true identity of an individual and control their access to all logical systems and physical facilities. To make that happen, smart cards or Common Access Cards (CACs) must be issued to agency employees and contractors, and must provide authentication to networks and applications based on the specific roles of individuals within the government. These cards should also do double duty by granting access to federal buildings in accordance with the user's security clearance level. They must interoperate with IT systems from multiple vendors. However, as you'd expect, they must be impregnable—unassailable by hackers, criminals and terrorists.

"This new standard will enable federal agencies to issue more secure and reliable forms of identification to better protect federal assets against threats such as terrorist attacks. It also will help safeguard against other risks such as identity theft."

-U.S. Commerce Secretary Carlos Gutierrez

Recommended Approach

When it comes to accessing facilities and information, security must be synonymous with identity management. An organization needs the ability to determine identity—*with certainty*—across all logical IT systems and physical facilities, enabling the appropriate level of access and the right connections 100 percent of the time. A low-level federal contractor, for example, must have extremely limited access to systems, applications, databases and facilities compared to federal employees with higher security clearances. This requires fine-grained, role-based access control that supports a wide variety of authentication mechanisms, including passwords, smart cards and biometrics.

Before an individual is authenticated to a network or admitted to a building, the computing infrastructure must have the real-time, autonomic intelligence to determine who that person is, what their relationship is to the agency or department, and what level of access their credentials entitle them to.

The infrastructure should also include the ability to track all access and use of resources through mechanisms such as auditing, time stamping and digital signatures in order to combat fraud, tampering, counterfeiting and terrorist exploitation. In every case, access must be based on strict adherence to policies established by HSPD-12 and other directives. At the same time, access must not get in the way of productivity; it must be quick and easy for those with the proper credentials. As a result, one of the most important design priorities for agencies will be to architect their identity infrastructure and select technology from the vendor community that will manage users' identities across heterogeneous IT environments. Lastly, the identity-driven security system should be easy to manage, while containing administrative costs.

By implementing an identity-driven approach, organizations can build a foundation to support compliance with HSPD-12 and other regulations, as well as address a number of other challenges that they may face in the future. Beyond security, a robust identity management solution can help governments meet operational challenges, improve citizen service and convenience, streamline intelligence gathering and sharing, and enable more informed decision-making.

Novell's Identity Assurance Solution for HSPD-12 SIN 132-62

Novell's Identity Assurance Solution for HSPD-12 is being deployed and tested in various agencies that are required to comply with HSPD-12 and PIV FIPS 201 requirements. Fundamentally, the Identity Assurance solution utilizes PIV cards to grant access to protected resources.

In November 2005, NIST invited potential vendors to provide products that support FIPS 201 Part II to NIST for the express purpose of including them in the PIV demonstration. NIST made the demonstrations open to all Federal agencies interested in FIPS 201 implementations. Participation required vendors to execute a Cooperative Research and Development Agreement (CRADA) with NIST.

In December 2005, Novell submitted its interest in providing its Novell Identity Assurance solution for inclusion in the NIST PIV demonstration and successfully demonstrated its HSPD-12 PIV solution at NIST in early June 2006.

The purpose of the PIV demonstration was to provide proof-of-concept demonstrations of commercially available products that support Federal Information Processing Standard 201 (FIPS 201) Part II. Additionally, the demonstrations showed the interoperability of NPVP certified PIV cards and PIV middleware.

Novell Identity Assurance Solution for HSPD-12 fits within the FIPS 201 functional model and interacts with PIV card vendors and component providers via a standard Personal Computer Smart Card (PCSC) interface.

Novell's Acquisition Submission to U.S General Services Administration

Novell has selected from the following GSA SIN 132-62 categories for our acquisition submission:

- PIV enrollment and registration services and products
- PIV system infrastructure services and products
- PIV card production services and products
- PIV card activation and finalization services and products
- Logical access control and physical access control services and products
- Approved FIPS 201 services and products
- Other professional services

PIV enrollment and registration services and products

Novell will provide the work flow for enrollment and registration, but it does not participate in biometric capture.

PIV system infrastructure services and products

Novell's Identity Assurance solution acts as the IDMS for the PIV system. This category fits us the best. We control the identity, the provisioning and de-provisioning of the identity and the association of a credential to an identity. We also manage the use of this credential to control access to various logical and physical systems.

PIV card production services and products

The Identity Assurance solution plays a part in card production. This will happen between card vendors such as ActiveIdentity and a service center.

PIV card activation and finalization services and products

The card activation can be seen as final personalization or the actual operation of pinning the card. Or this may mean that the card is active for use in PACS & LACS. Novell would need clarification from GSA before we commit to a response within this category.

Logical access control and physical access control services and products

Novell's Identity Assurance solution provides logical access control with eDirectory and will be pushing information to PACS. Being the hub as IDMS, we fall into this category as enabling PCS and LACS.

Approved FIPS 201 services and products

Novell Identity Assurance Solution for HSPD-12 fits within the FIPS 201 functional model and interacts with PIV card vendors and component providers (such as ActiveIdentity) via a standard PCSC interface.

Other professional services

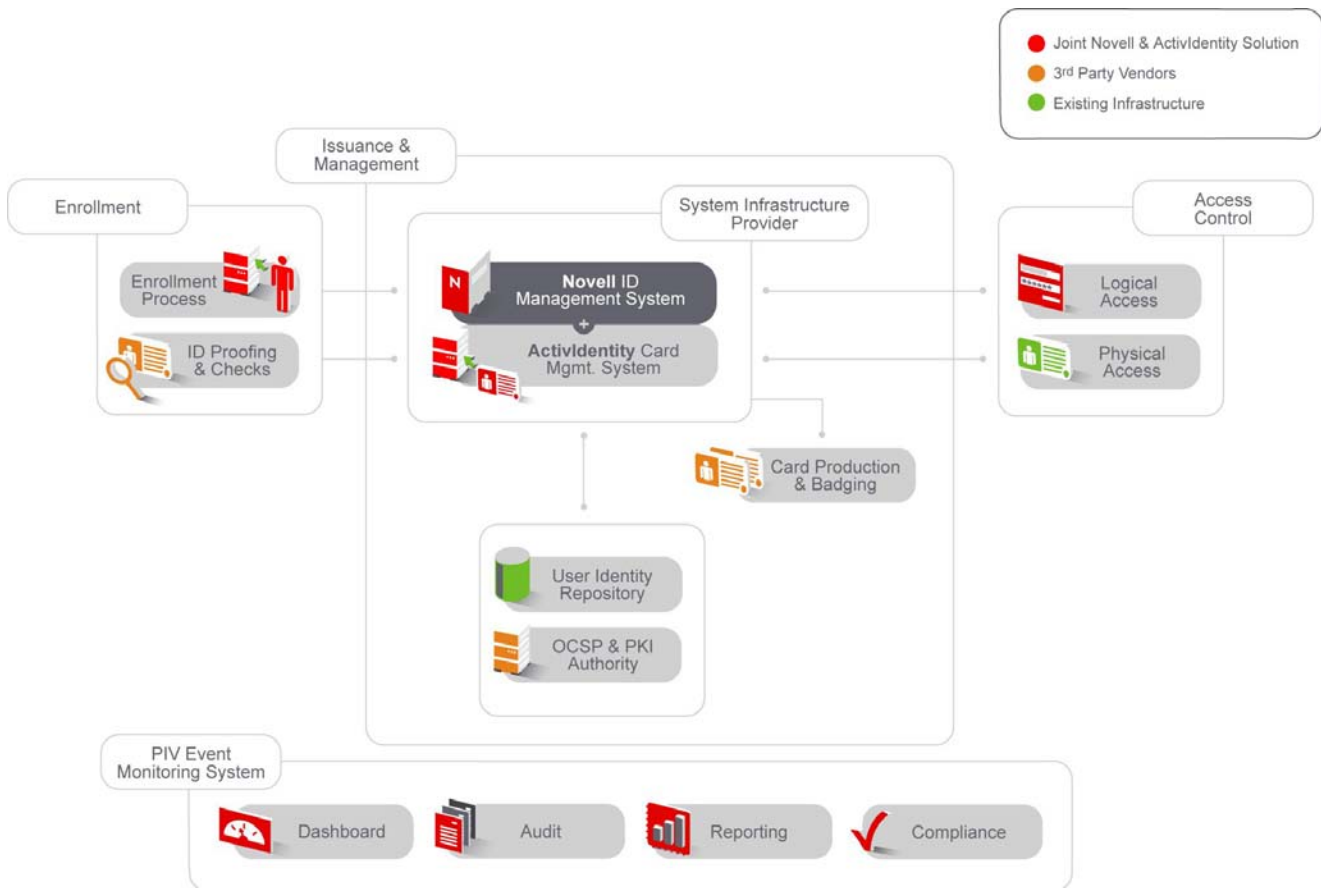
Novell provides worldwide IT consulting, training and support services to address our customers' needs. Our worldwide IT consulting practice provides the business knowledge and technical expertise to help our customers implement and achieve maximum benefit from our products and solutions. We also offer open source and identity driven services that are focused to aid our clients in rapidly integrating applications or migrating existing platforms to Linux.

HSPD-12 Solution Architecture Overview

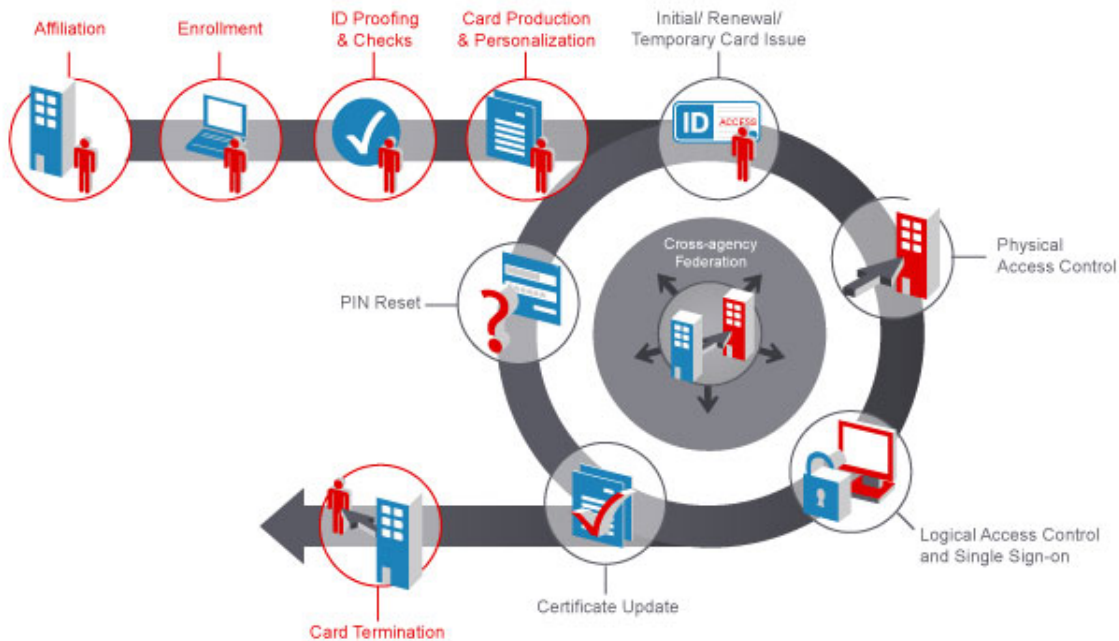
Novell, with its Identity Assurance solution and strategic partnerships, is uniquely positioned to fulfill the requirements for a HSPD-12 PIV solution across the five categories:

- Applicant enrollment and registration
- Smart card production
- Smart card personalization
- Card issuance and management
- PKI certificate issuance and management

The Novell Identity Assurance Solution for HSPD-12 PIV-II is comprised of four key sub-systems: 1) Enrollment, 2) Card Issuance and Maintenance, 3) Physical and Logical Access Control and 4) Event Monitoring and Management:



The Novell Identity Assurance Solution for HSPD-12 PIV-II is designed to streamline PIV life cycle activities by integrating external systems such as vetting or background verification systems, card management systems, certificate authorities, card production systems, logical IT access control systems, physical access control systems, etc.



In addition to fulfilling the complete requirements of a HSPD-12 PIV-II solution, Novell offers an optional Event Monitoring & Management sub-system to provide greater visibility to PIV-related events to ensure system-level security and compliance.

The following sections describe the sub-systems, options, and processes included in the Novell Identity Assurance Solution for HSPD-12 PIV-II.

Enrollment and Registration

The PIV card issuance process starts with a sponsor who initiates a request to issue a PIV card. The Enrollment sub-system detects this event and sends email notification to the new applicant along with instructions to gather and complete appropriate documentation. The applicant is requested to schedule a meeting with a registrar who then captures the identity information and submits it for verification through a vetting process. The registrar manually completes steps to confirm the identity of the applicant against the documentation presented and uses the Novell Identity Management User Portal, along with the 3rd party vetting systems, to enter Identity information including I-9 form, finger prints, facial images, etc.

The Enrollment sub-system is designed to support integration with 3rd party systems such as Daon, Viisage, Lenel, EDS, etc., in a standards-based way. The process can also include integration with existing HR or contractor management systems. Novell Identity Manager has drivers that integrate with over 200 external systems including common human resource information systems. Once registration information is submitted, the Issuance Officer is notified to start the card production process. The business processes included in the PIV solution are flexible and can be customized.

Card Issuance and Maintenance

The card issuance process is designed to support the creation of a PIV card for federal employees and contractors who have successfully completed the identity verification process or need to be issued a provisional card based on individual agency guidelines. The issuance process is initiated by the workflow, which takes enrollment information and passes it to the Card Management system (CMS), ActiveIdentity CMS 4.0, which is included as part of the Novell Identity Assurance solution. The card management system then creates a data packet that contains the identity information as well as a digital certificate that can be obtained from vendors who participate in the PKI federal bridge (Verisign, Cybertrust, Entrust, and Microsoft). This data packet is then sent to a card production and badging station for card creation. Once a card is created, the workflow updates the IDM system to indicate the status and notifies the applicant to schedule a meeting with the issuing officer. The applicant receives their personalized card and securely receives their PIN. Once the PIV card is issued to the applicant, the PIV card unique identifier is captured in a central repository that holds the identity profile for the federal employees or contractors and their associated PIV card identification.

The card issuance and maintenance systems are also designed to support typical life cycle maintenance processes including the following:

- Card issuance
- Card replacement and temporary card issuance
- Card termination

The Novell Identity Assurance Solution is designed with extensibility in mind. In addition to meeting PIV solution requirements, this solution can easily be extended to integrate with employee and contractor systems of record (a.k.a. authoritative data sources) and provision them to the appropriate physical and logical IT systems based on their role. In addition, this solution can be further extended to support typical employee and contractor life cycle activities such as the following:

- Employee or contractor termination
- Employee role changes (transfers between departments / locations, etc.)
- Employee information changes (name, address, etc.)

When a federal employee or contractor is terminated or fails the vetting process, their access rights are revoked instantaneously and the card management system receives instructions to terminate the card. Upon receiving this notification, the CMS system disassociates the user from the card and revokes the digital certificate on the PIV card rendering it invalid.

Logical and Physical Access Control

The Logical & Physical Access Control sub-system is responsible for enforcing access control policies at run time when the federal employee or contractor tries to access the logical IT systems or physical facilities. Access control policies are enforced based on the federal employee or contractor identity and authentication credentials stored on the PIV card issued by the card issuance and maintenance sub-system.

Event Monitoring and Management

The Event Monitoring and Management sub-system is an optional component of the Novell Identity Assurance Solution for HSPD-12 PIV-II.

The PIV event monitoring system provides a flexible and scalable solution to capture events that are triggered during the PIV card life cycle activities. This system provides a set of reports that

Novell HSPD-12 Positioning Paper & PIV Solution Overview

allows authorized users to see the state of the PIV processes in real time; it can also be extended to support enterprise-level security event monitoring and management needs as well audit and compliance reporting requirements. Custom reports and graphs to monitor a variety of conditions can also be created.

Appendix A. Novell HSPD-12 Solution Overview

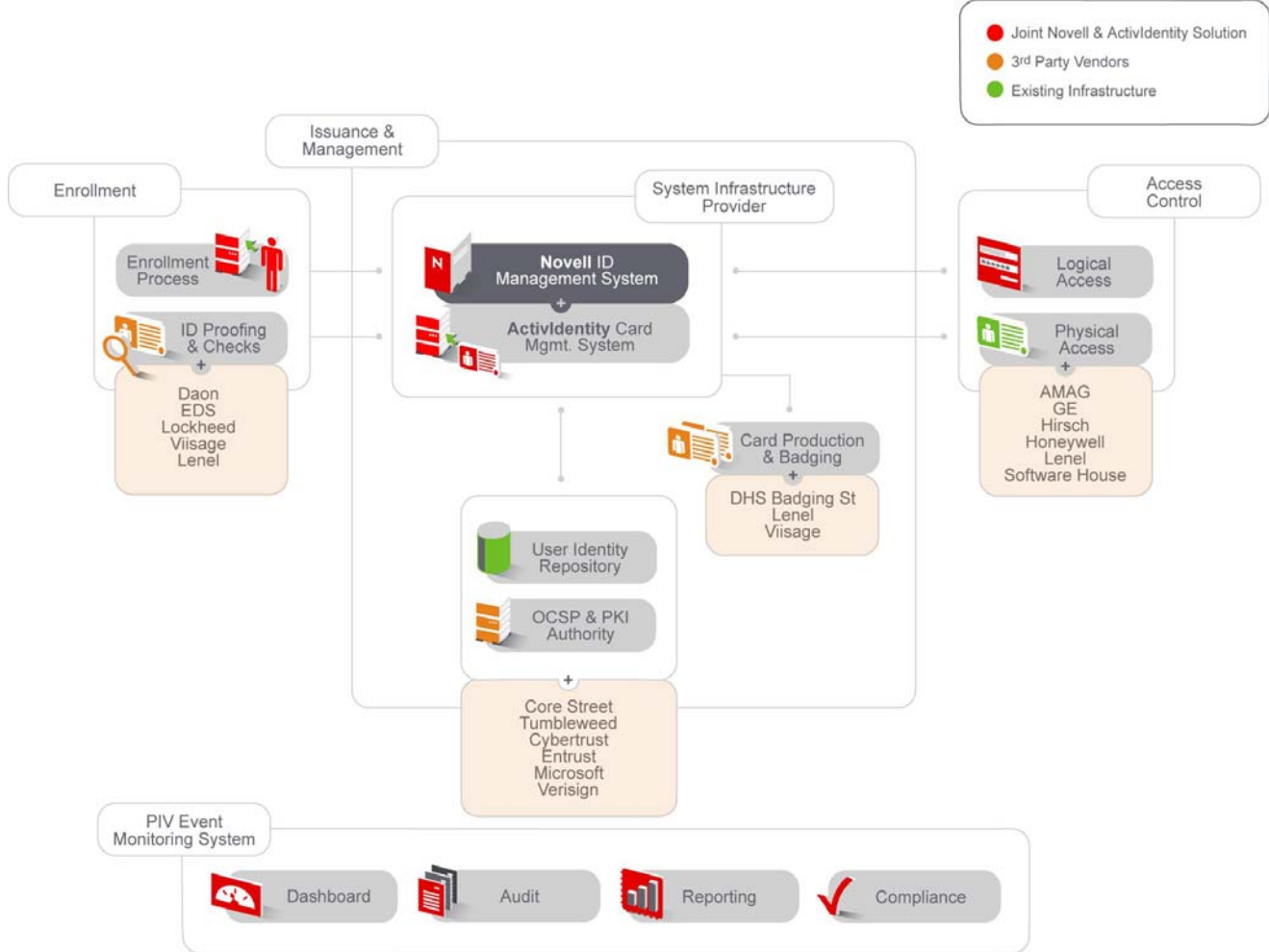
Description

The PIV solution from Novell is built on a strong business process management (BPM) foundation that streamlines the business processes involved in PIV life cycle activities as well as traditional employee access management activities. The BPM foundation is designed to support business processes between IT systems as well as processes that involve people (for example, the PIV card sponsor, enrollment officer, etc.). In addition, this BPM foundation provides the ability to integrate with internal and external 3rd party systems in a standards-based way.

Novell Identity Assurance solution can be integrated with a number of 3rd party vendor systems that are required to implement a fully functional HSPD-12 PIV solution for the federal agencies. The table below provides a partial list of these key 3rd party systems:

<i>Enrollment</i>	<i>PKI</i>	<i>Badging</i>	<i>Access Control</i>
Daon	Corestreet	DHS Badging St	GE
EDS	Tumbleweed	Lenel	Hirsch
Lockheed	Cyberstrust	Viisage	Honeywell
Viisage	Entrust		Lenel
Lenel	Microsoft		Software House
	Verisign		

The figure below identifies the points of integration with 3rd party systems in the context of the overall HSPD-12 PIV Solution Architecture:



The HSPD-12 Solution from Novell is designed to:

- Automate the full range of PIV life cycle activities by integrating people, processes and technologies
- Support interoperability between agency-specific HSPD-12 PIV solutions through open standards
- Provide a unified solution for physical and logical access control through a common identity assurance platform
- Enable Role-Based Access Control (RBAC) and enforcement of Separation of Duties (SoD)
- Provide a highly secure, scalable and reliable architecture by leveraging an industry-leading, proven directory services foundation
- Offer real-time monitoring and management of PIV life cycle activities and related security events
- Provide the flexibility and extensibility required to implement a cost-effective HSPD-12 PIV Solution and leverage investments in existing IT systems, related processes and people.

The role of Identity Management within the Identity Assurance solution for HSPD-12

Novell understands the requirements as outlined within the Qualification Criteria provided by the GSA. As the identity management solution leader, it is our experience and technical superiority that we offer for the HSPD-12 PIV project. Our goal is to establish long-standing and trusted technical partnerships with those we work with on this initiative, and we do this by leveraging our

experience and knowledge of the business and technical activities of customers to ensure that our solution specifically meets our customer's needs.

Just recently InfoWorld, Network Computing, Burton Group, Gartner, and Meta Group all recognized Novell as the leader in the Identity Management space. Novell is accelerating that leadership and is uniquely positioned in the market to provide a comprehensive, standards-based, COTS solution for the HSPD-12 initiative.

In the area of Identity Management and HPSD-12, Novell offers three distinct and tangible advantages that no other vendor can provide:

- 1) Unparalleled knowledge of identity management technology, especially in government environments;
- 2) Methodologies and utilities developed in the execution of projects similar in size and scope to this project; and
- 3) Experience. Novell has provided directory-based identity management provisioning solutions longer than any other vendor in the market.

In our HSPD-12 PIV II solution, Novell maximizes the use of its best-of-breed technology to provide a flexible yet highly secure solution to establish the required security infrastructure and foundation for your requirements.

Acronyms Used

- IDRPS: Identity Registration and Proofing System
- CMS: Card Management System
- CPR: Card Production Request
- CRR: Card Revocation System
- MOC: Match On Card
- PIV: Personal Identity verification

System Descriptions of IDMS and CMS

The Identity Registration and Proofing System (IDRPS)

The IDRPS relies on an IDMS. This database stores enrollment and validation data such as demographic information, identity traits, background check results, signatures and copies of original ID documents, and the PIV card status of all Applicants who have either been already issued a card or who are eligible to receive a card, i.e., are undergoing vetting. This enrollment and validation data includes elements that will be written to/onto the Smart Card, or will be used to populate other mandatory Smart Card fields that are also stored in the IDRPS and created in the FIPS 201 PIV Card Issuance and Maintenance process. They include access strings (the CHUID and bar codes), and the photograph of the Cardholder, among others.

Card Management System (CMS)

CMS is the PIV card issuance and maintenance (including card accountability) component of the PIV1 system. The CMS provides a FIPS201 – PIV-I compliant, secure auditable, and scalable platform for issuing PIV Cards with PIV-II (800-73) compliant transitional card edge and data model including the PKI. CMS also allows for the initialization and personalization of non-PIV applications on the card and provides PIV card inventory functionality for complete card accountability for both issued and unissued

cards. In a post issuance mode, CMS manages the post-issuance life cycle of the PIV card and credentials such as PKI keys and certificates. This includes card and credential revocation, replacement, and PIN management services. Finally, CMS provides a fully documented API, which provides the necessary flexibility to allow easy integration with IDMS.

Functional Interface Description

Issuance Use Case

Step	IDMS	CMS
1	IDMS captures and processes all enrollment data from the enrollment workstation.	
2.	IDMS generates agency unique data elements.	
3.	IDMS segments 10 flat fingerprints and selects two fingerprint bio images for PIV card encoding in 800-76 template format and, optionally, other Match-on-Card template formats.	
4.	IDMS converts photograph and bio templates to Base64 text format.	
5.	IDMS initiates User Record creation in CMS (Life Cycle Mgmt API).	CMS Creates a cardholder record.
6.		CMS notifies IDMS of success/failure of cardholder creation (Life Cycle mgmt API).
7.	IDMS creates Card Production Request data package, digitally signs package, and then transmits to CMS (Life Cycle Mgmt API) Note: Digital signature not implemented in the current PIV-0 Test Bed.	CMS receives card request data package and performs the following: 1. Calls the Enrollment Plug-in to parse the XML header values to be stored in the CMS table. 2. Validates digital signature 3. Validates file syntax 4. Encrypts the XML file 5. Loads XML enrollment data file into the LDAP Directory

Step	IDMS	CMS
		Note: Steps 2-4 are not implemented in the current PIV-0 Test Bed.
8.		CMS notifies IDMS of successful/unsuccessful receipt and validation of CPR data package (Life Cycle Mgmt API).
9.	IDMS creates validated CMS Card Issuance request and transmits to CMS (Life Cycle Mgmt API).	CMS receives request, creates a validated issuance request.
10.		CMS notifies IDMS of successful/unsuccessful validated issuance request creation. (Life Cycle Mgmt API).
11.	IDMS initiates approval of the validated CMS Card Issuance Request and transmits to CMS (Life Cycle Mgmt API).	CMS receives request, approves the validated issuance request.
12.		CMS notifies IDMS of successful/unsuccessful CMS Card Issuance Request approval. (Life Cycle Mgmt API).
13.	IDMS receives CMS notification; if notification is affirmative, IDMS updates issuance state as pending; if notification indicates a failure, IDMS generates an error.	
14.		<p>Card Issuance:</p> <ul style="list-style-type: none"> • CMS Operator logs in to Issuance Workstation to issue a PIV Card to Applicant. • Applicant performs a 1:1 biometric check to validate their identity. • Operator initializes and personalizes the PIV card. <p>After card chip personalization is complete, CMS notifies IDMS of card issuance event (Notification Plug-In API).</p> <p>Optionally, the PIV Card can be produced in</p>

Step	IDMS	CMS
		batch mode, prior to the issuance. Upon completion of the card production in batch, CMS sends a notification to IDMS that the PIV card has been produced. (Notification API) IDMS can then schedule an appointment with the Applicant for Card Pick-up. Note: Batch processing is not implemented in PIV-0 Test Bed.
15.	IDMS receives CMS notification; if notification is affirmative, IDMS updates issuance state as "issued"; if notification indicates a failure or no notification acknowledgment is received, IDMS generates an error and seeks instruction on how to proceed.	

Revocation Use Case

Step	IDMS	CMS
1	IDMS receives PIV Card revocation request.	
2.	IDMS creates card revocation request (CRR).	
3.	IDMS digitally signs CRR.	
4.	IDMS transmits CRR to CMS (Life Cycle Mgmt API)	CMS receives signed CRR, verifies signature and contents are properly formatted and have not been altered Note: This feature is not implemented in current PIV-0 Test Bed.
5.		CMS processes CRR request and revokes the specified PIV Card; (CMS proceeds to terminate all PKI certs).
6.		CMS notifies IDMS that CRR has been successfully completed (Notification Plug-In

Step	IDMS	CMS
		API) Note: This feature is not implemented in current PIV-0 Test Bed.
7.	IDMS received CMS notification; if notification is affirmative, then IDMS updates issuance state as Revoked; if notification indicates a failure or no notification acknowledgment is received, IDMS generates an error and seeks instruction on how to proceed.	

Appendix B. HSPD-12 Professional Services

Novell Integrated Services

Novell is a product and services company with a history of delivering high-reliability solutions. Our products have impressive features and functionality; however it is our integrated support, service, training and consulting services that ultimately set us apart from the competition.

Novell has more than 20 years of experience as a strategic solutions provider to national, state and local governments around the world. Our strategy has been to develop identity-based technologies as a set of standards-based, discrete services, as opposed to monolithic applications dependent upon the use of proprietary underlying technologies. Our professional services are based on understanding the complexities our customers face in the information economy and the way our products best enable success in our customers' environments. We focus our consulting and training expertise on identity-driven solutions such as HSPD-12, and provide a full range of support services for all proprietary and open source products offered by us.

We partner with the industry's leading independent software vendors, systems integrators, and original equipment manufacturers to enhance the value delivered to customers. We deliver solutions through a multi-channel strategy, serving large organizations directly, partnering with systems integration partners or supporting small and medium organizations through our channel partners. To maximize our reach while ensuring the highest quality of service to our customers, we provide our strategic partners complete access to all of our tools, training and methodologies.

HSPD-12 Planning, Design and Deployment Expertise

Many organizations are anxious to rapidly move forward in addressing the technical and business issues related to HSPD-12, but are not sure where or how to start. Recognizing that a solid planning effort speeds implementation and reduces risks, savvy organizations are turning to a proven identity management consulting partner for help in the planning process.

The Novell Integrated Services organization employs professional identity management consultants, technical architects, technical service engineers, business strategists, project managers, trainers, and other skilled resources to provide full lifecycle support. Our HSPD-12 consulting methodology is comprised of 2 parts: HSPD-12 Preparation and Solution Validation and Migration Services

HSPD-12 Preparation and Solution Validation

Because many organizations may need help determining how best to meet HSPD-12 requirements, Novell uses a Discovery and Road mapping methodology. This methodology helps organizations develop an integrated HSPD-12 strategy and plan, from both a technology perspective and a business perspective. Working with the client, Novell identifies key goals, assesses gaps and dependencies, prioritizes initiatives and actions, and integrates the next steps in a phased roadmap. This paves the way for successful implementation and speeds time-to-value.

HSPD-12 Preparation & Solution Validation

Novell's Rapid Approach to Creating Your Agency Plan

Overview

Educates and aligns stakeholders. Helps client prepare to implement an HSPD-12 solution spanning people, process and technology areas. Assembles Agency Plan. Provides a springboard for successful implementation.

Benefits

- Educates and aligns stakeholders
- Develops an understanding of the HSPD-12 requirements (process, people and technology)
- Defines a solution for HSPD-12 compliance (people, process and technology)
- Creates a clear Agency Plan for moving forward

Sample Deliverables

- Common understanding of HSPD-12 PIV I and PIV II requirements (as applied to your agency)
- Inventory of current access control policies (PIV I) and impacted infrastructure (PIV II)
- Compliance Gap analysis (PIV I and II)
- Decisions on future access control policies (PIV I) and high-level future technical architecture (PIV II)
- Prioritized inventory of objectives to become compliant with PIV I and II (and prioritized high-level requirements for each objective)
- Define Roadmap for Implementation of HSPD-12 and defined next steps
- Define Statement of Work and Project Work Plan
- Assemble Agency Plan for OMB Review

HSPD-12 Migration Services

Novell's HSPD-12 migration services are comprised of: three primary areas (captured in the following slides):

- Design, Develop and Test
- Train and Deploy
- Transition and Control

Design, Develop and Test



Overview

Executes the Roadmap for business process and technology components of the solution by reviewing and tuning the Architecture against scope objectives. Designs, develops and tests the solution.

Benefits

- Ensures business process changes (PIV I) are identified, designed and developed in conjunction with technology changes (PIV II)
- Operational and technical risks are identified and mitigated
- Solution is certified for deployment

Sample Deliverables

- Scope of PIV II functionality
- Standards and naming conventions
- Design specifications for technical components
- Test conditions and testing procedures
- Security Accreditation (FIPS 201 and PIV II)
- Tested components
- Updated Agency Plan for OMB review

Train and Deploy



Overview

Finalize and Test performance, business process, metrics, training modules and reporting tools to ensure compliance with FIPS 201 and PIV II requirements.


Benefits

- Organizational support for business process changes introduced by solution
- Reduce the risk of production roll-out through extensive testing and piloting
- Ensures compliance with FIPS and PIV II requirements

Sample Deliverables

- Overall Migration & Deployment Plan
- Executed Communications Plan
- Training Modules & Executed Training for Stakeholders
- Solution Test (against test conditions and FIPS requirements)
- Updated Risk Analysis & Mitigation Plan

Transition and Control



Overview
Transitions the deployed solution into a production environment for HSPD-12 operational requirements. Documents processes and best practices for future reference. Introduces management reporting processes to monitor continued compliance and make adjustments as necessary.

Benefits

- Continual maintenance & optimization of solution technology
- Assessment of solution business value
- Use & ownership of solution by stakeholders

Sample Deliverables

- Deployed in Production environment
- Documented processes, learnings and best practices
- Management reporting processes and logs
- Feedback mechanism for continual improvement including HSPD-12 Governance Model

Training

In addition to a variety of end-user training offerings (e.g., classroom, online live instruction, CBT modules, quick reference cards) Novell offers in-depth Security/ Identity & Access Management training for the system administration and technical teams managing and supporting the HSPD-12 solution. For detailed information regarding Novell Security/Identity & Access Training Services, please visit: <http://www.novell.com/training/bytopic/ident.html>.

Ongoing Service and Support

Novell offers Premium, Remote and Managed Services that provide proactive HSPD-12 solution support and monitoring—and even onsite management—to ensure systems are always running smoothly.

Premium Service is a tiered model of support offerings that allow agency clients to select the level of support that makes the most sense. Regardless of whether there is a mix of traditional and new Novell technologies, Premium Service ensure products run reliably. Depending on the level of service, the following benefits are available:

- Priority access to expert resources, 24x7x365
- Fast and predictable response times
- Dedicated resources for personalized support
- Relationship management
- Access to industry-leading support tools

With multiple levels of service, plus many optional services, our federal clients can choose the support program that best fits their organization - from occasional telephone support to dedicated

support engineers who bring full-time support, knowledge and expertise to agencies' mission critical or highly customized solutions.

Benefits

Dedicated Resources				ASE	PSE	DSE
Account Management			Service Account Manager	Service Account Manager	Service Account Manager	Service Account Manager
Access	12x5	24x7	24x7	24x7	24x7	24x7
Call Center Incidents	10 incidents	25 incidents	50 incidents	50 incidents	50 incidents	50 incidents
Maximum Response Time	4 hours	2 hours	1 hour	1 hour	30 minutes	15 minutes
Tools & Training	1-Support Res. Library 1-eDirectory Toolkit 1-Education Voucher	1-Support Res. Library 1-eDirectory Toolkit 2-Education Vouchers	1-Prof. Res. Suite 3-Education Vouchers	1-Prof. Res. Suite 5-Education Vouchers	3-Support Res. Library 2-Prof. Resource Suites 6-Education Vouchers 1-BrainShare Pass	6-Support Res. Library 3-Prof. Resource Suites 10-Education Vouchers 2-BrainShare Passes
	Premium 1000	Premium 2000	Premium 3000	Premium 3000 ASE	Premium 4000 PSE	Premium 5000 DSE

Customized Configuration ►►

Higher Level of Service & Personalization ▲▲

Novell Remote and Managed Services offer the following services:

Remote Health Checks—provides a one-time health check or periodic health checks sold as an annual subscription. Novell uses its secure dial-in technology to remotely assess system performance and provide alerts for potential problems.

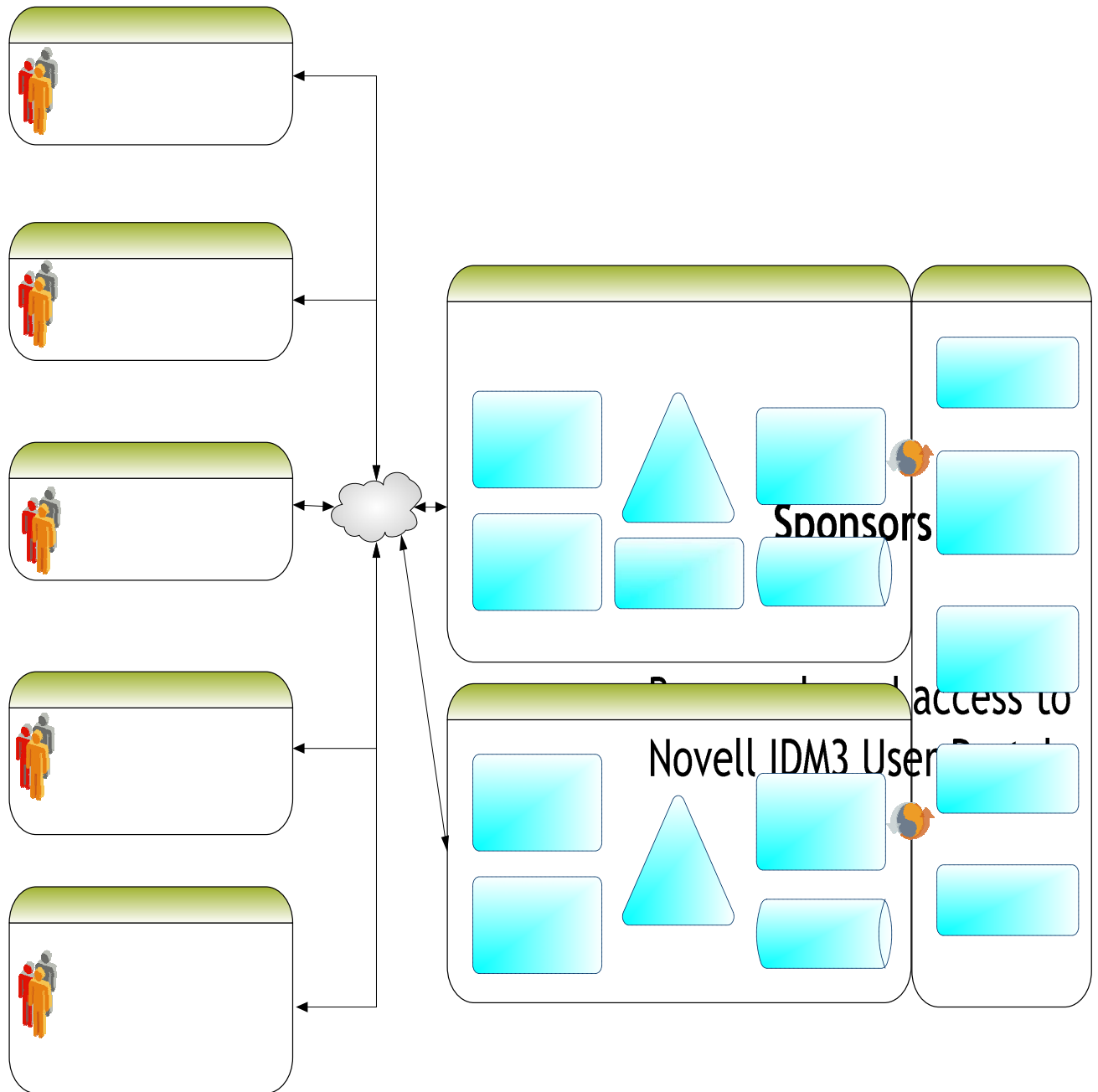
Remote Monitoring—includes daily health checks and up to 24x7 monitoring of selected systems. Novell also provides escalation routing and status reporting.

Managed Services—includes both health checks and monitoring, as well as Novell Technical Services engineers who proactively manage any system issues. Novell provides an uptime guarantee at this service level.

With Novell Remote and Managed Services, clients are freed from the daily—and often impossible—task of monitoring and managing their systems so that IT staff can focus on core agency initiatives.

In every case, the Novell Integrated Service organization stands ready to provide assistance at every step of the way—from initial HSPD-12 planning, to onsite knowledge transfer and implementation, to post-implementation training, support, maintenance and managed services.

Appendix C. Enterprise Deployment Architecture



Applicants

Access to email to receive notifications on steps to complete to receive DOL PIV card

Appendix D. Roadmap for Identity Assurance Solution

Required Components

- .Card Issuance & Management System
 - Enrollment/registration workflow
 - Identity proofing
 - Key management (PKI, Certificate Authority)
- .Access Control System
 - Physical Access Control (identity, authentication, authorization)
 - Logical Access Control (identity, authentication, authorization)

N

2 © Novell Inc. Confidential & Proprietary

