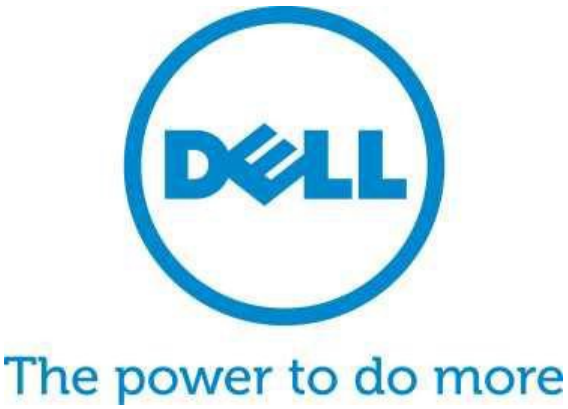
Dell Mobile Clinical Computing VMware® View Solution

A Dell Technical White Paper



November 2012

Contents

Audience

This white paper is intended for test engineers, architects, and IT administrators involved in the decision making process for the planning, configuration, and operation of a desktop virtualisation solution in a Healthcare environment. This document is also intended to assist solution architects in planning, design, and deployment of the Dell Mobile Clinical Computing (MCC) solution.

Introduction

Today's dynamic healthcare environment relies heavily on the latest technology to increase the speed and accuracy of patient diagnosis and treatment. Healthcare professionals are required to interact with a range of end point devices to access medical applications that are hosted locally or on servers in a centralised data center. Interaction with end points has historically presented a challenge because each device may not have all of the necessary applications available. As a result, healthcare professionals may have to wait to use a specific end point, potentially delaying patient care. The process can be further delayed by security and compliance regulations which require all users to first provide credentials for each application, then log out of individual applications and from their user session when they leave each exam room. Over the course of a typical workday, these processes can seem increasingly cumbersome and time consuming leading some healthcare professionals to skip the log off process altogether. Fortunately, **Dell's Mobile Clinical Computing (MCC)** solution addresses these issues and mitigates many of today's key challenges:

- Limiting the amount of time clinicians and nurses spend searching for available end points as well as the time spent accessing and then re-accessing applications;
- Providing a single sign-on instance that clinicians and nurses can use to authenticate seamlessly against endpoint and multiple applications;
- Providing quick and secure access to patient information on-demand using proximity and/or biometric authentication methods;
- Reducing and limit the time spent by IT staff managing client systems in their environment

Dell's MCC enables medical professionals to leverage the benefits of desktop virtualisation in a way that encourages the right security behaviour without impeding clinical workflow. MCC's desktop virtualisation and identity access management features enable single sign-on and strong authentication allowing caregivers to log in or approach a terminal and be presented with a desktop that delivers the applications and patient information they need without requiring additional authentication for each application or each application layer. Caregivers can log into end points in patient exam rooms or anywhere in a hospital seamlessly, allowing them to spend more time with patients, see more patients per week (and per year), and provide a higher level of service.

In fact, in another whitepaper as a result of trials we've run in Europe, we've actually proven that our MCC solution in a live clinical workflow can deliver*:

- Up to 215+ minutes per user per week productivity gain (9% improvement)
- Economic value of productivity can be up to £10,000 per user per annum
- Appropriate Information Security delivered that's workable for users
- Improved patient safety, quality of care and patient satisfaction

Dell Mobile Clinical Computing (MCC)

Healthcare is an ideal use case for desktop virtualisation given the combination of several requirements and pain points: (1) the need for fast access to applications like EMR, (2) the critical need for secure data, (3) unique user situations and applications, (4) the data security risks introduced by consumer devices such as tablets and smartphones, and (5) IT departments' wish to simplify complex requirements and serve demanding (and potentially adversarial) end user dynamics. This created an opportunity for Dell to provide a flexible solution to serve the specific tailored needs of the healthcare sector and deliver an enterprise class solution that provides enabling technology as well as key clinical workflow features with a compelling end user experience.

Dell Mobile Clinical Computing Solution (MCC) is a desktop virtualisation and identity access management solution for healthcare professionals to securely access applications, data, anywhere from nearly any device. Healthcare organisations are looking to enable improved productivity for caregivers while complying with strict information management standards designed to protect patient privacy. Dell MCC solution provides healthcare professionals with flexible computing enhancements such as increased security, on-demand access to applications and information, the ability to stay connected while roaming, 24x7 availability, and increased computing power. At the same time, MCC provides IT departments with the ability to securely centralise control of all end-user data and images while enhancing end user flexibility and mobility. By enabling a digital identity with application, desktop, and user profile virtualisation, caregivers can access applications and data from any device, freeing up more time to deliver better patient care. MCC offers key benefits healthcare providers are looking for including:

- **Data Security:** Information is stored in the data centre – not on the endpoint device – thereby reducing the risk of lost or stolen data. Multi-factor authentication helps prevent unauthorised access.
- **Clinical Efficiency:** Single sign-on solutions enable fast login to applications thus reducing time to access patient records and other associated data. Proximity cards or contact access smartcards provide easy clinician single sign-on authentication. Roaming session transfer enables access to a virtual desktop from any location and a range of end points. No device dependency and follow-me printing provides location flexibility regardless of the device.
- **IT Productivity:** Dynamic provisioning of user applications and data simplifies deployment and provisioning of new virtual desktops. Centralised control of virtual images simplifies application upgrades and ongoing maintenance.

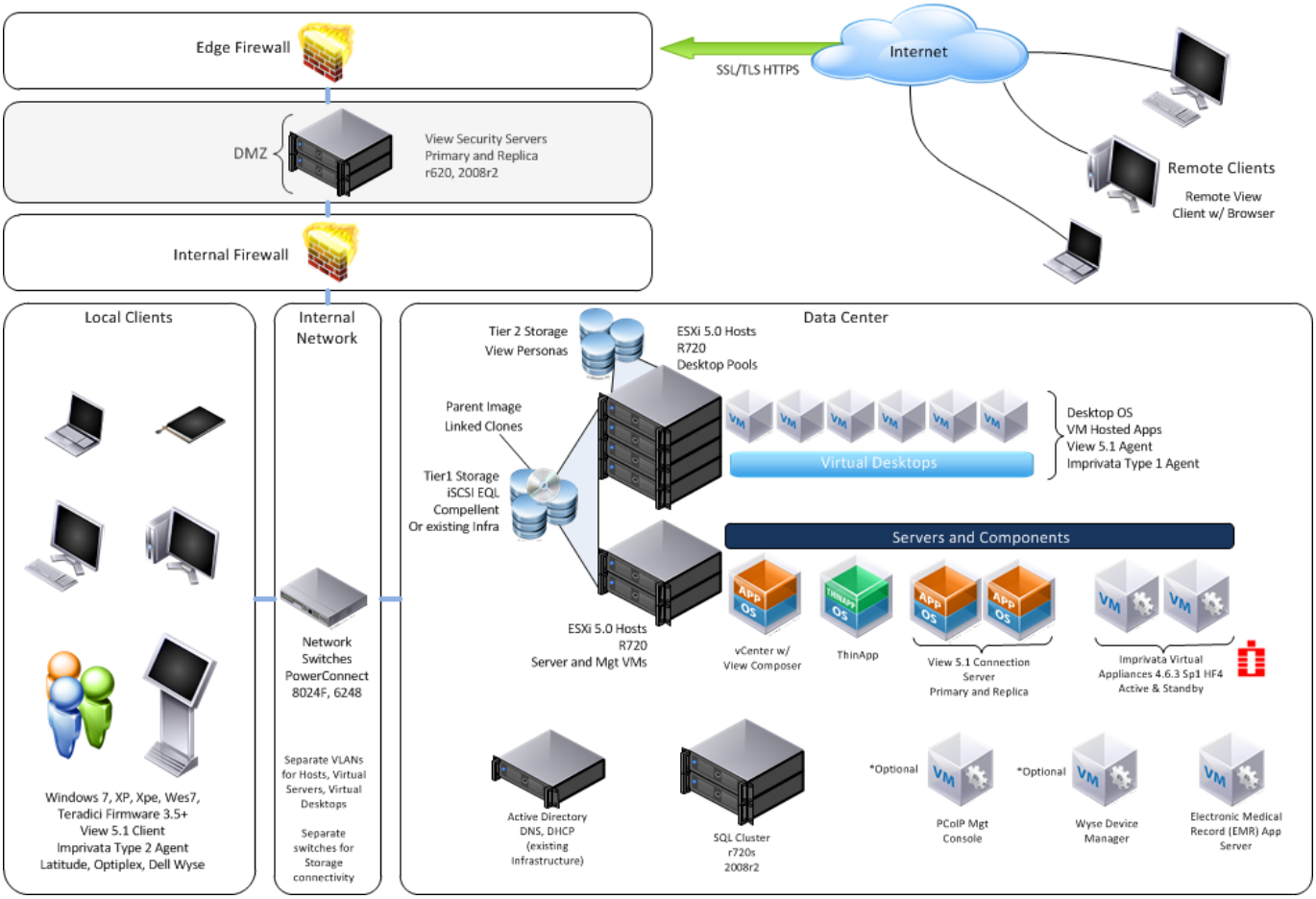
Below are the key features of Dell MCC solution that enhance data security, clinical efficiency, and IT productivities for healthcare organisations:

- Delivery of the correct resources quickly, on-demand, regardless of location or device.
- Acceleration of user access via ID badges, fingerprint biometrics, and smartcards, where credentials are governed by IT role-based access definitions.
- Seamless and time-bound transfer of session credentials and user data from one workstation logon instance to another, supported via badge or fingerprint login, allowing users to retain session state on a different device.
- Seamless redirect of print jobs to the printer closest to the user's terminal.
- Auto-launch of applications defined per user profile.
- Single sign-on capability applications removing the need for users to remember or input multiple different passwords
- Customisation of desktop environment per user profile.
- Combine any two of the MCC-supported authentication methods to enable multi-factor authentication, which helps compliance with healthcare industry privacy and security rules and regulations (e.g. HIPAA, PCI).
- User ease of use.

Reference Architecture

Dell's MCC VMware View Solution is built on top of the DVS Enterprise 6020 solution and powered by the latest Dell 12G servers. The reference architecture includes session brokering, role-based user workspace and application access, single sign-on, automated application launch, proximity or smartcard authentication, session roaming, and fast user session switching on client devices meeting criteria defined. The user's desktop experience, consisting of operating system, applications, and data are moved from client devices to the data centre by implementing application virtualisation and desktop virtualisation technologies. The solution provides centralised control of end-user data, applications, and operating system(s) while maximising client-side flexibility and allowing end-user access both locally and remotely to user-specific corporate desktop or Dell client systems.

Figure 1: Dell MCC VMware View Solution Reference Architecture Diagram



Dell MCC VMware View Solution is offered in rack or blade server configurations with flexible options for Tier 1 and Tier 2 storage on local and/or Dell EqualLogic or Compellent storage. Dell EqualLogic storage platform allows for automatic load balancing, tiering, snapshots and replication. Below Tables 1 below illustrates a sample configuration to implement a customer environment of 500 concurrent users with Dell 12G servers both in rack and in blade form factors and EqualLogic storage:

Table 1: Sample 500 Concurrent Users Configuration

500 Concurrent Users	Rack Configuration	Blade Configuration
High Availability Infrastructure	6 Client Host Server: PowerEdge R720 2 Mgmt Server: PowerEdge R720 T1 storage: Local Storage 2 ToR Switch: PowerConnect 8024F	1 Blade Enclosure 6 Client Host Server: PowerEdge M620 2 Mgmt Server: PowerEdge M620 T1 storage: 1 EqualLogic PS6110XS Blade Switch: 2 PowerConnect M6348, 2 PowerConnect 8024-K 2 ToR Switch: PowerConnect 8024F
Virtualisation Software	500 VMware View 5.1 Premier Dell Edition licenses Including View Persona Management AlwaysOn Desktop (optional for additional DR and HA)	
Identity Access Management Software	2 Imprivata OneSign Appliances (option for physical or virtual, virtual shown in figure 1) 500 Authentication Management & Single Sign On licenses Secure Walk-Away™: and OneSign Self-Service Password Management™ optional (see page 14)	
Multi-factor Authentication*	Password, Pin, Proximity & Smart Card*, Biometric (*Smart Card examples shown in Appendix 1.0, pg.24)	
Endpoint Devices	Dell Wyse Zero Clients (PCoIP or RDP), Thin Clients (WES 7) Dell Latitude & OptiPlex	
Management Software	Dell Wyse Device Manager (WDM)	

**smartcard readers are hardware dependent and not included*

Dell Desktop Virtualisation Solution (DVS) Enterprise

The foundation of Dell MCC VMware View Solution is Dell's Desktop Virtualisation Solution (DVS) Enterprise architecture which is built on the new 12th generation (12G) of Dell PowerEdge server family and VMware vSphere & View 5.1.

Dell PowerEdge 12G servers are designed with more memory capacity and more integrated I/O (input/output) than the previous generation. This increased capacity is crucial for virtualisation performance and scalability. With multi-core Intel® Xeon® processors, increased DIMM slots, PCIe Gen3 expansion slots and the ability to embed the hypervisor on secure digital (SD) card or internal USB, hospitals can now maximise the number of virtual machines per server and gain fast results from their virtualised environment. Indeed, Dell's 12G servers can provide up to 18 times more Microsoft® SQL Server® transactions per second when using PowerEdge Express Flash Storage solid-state drives (SSDs) (directly connected to the CPU and memory bus).

These PCIe (PCI Express) SSDs help to accelerate database, application and I/O (input/output) performance, enabling health care professionals to turn data into valuable information faster. Next-generation Dell PowerEdge servers raise the bar on IT efficiency and help healthcare organisations embrace innovation in their IT environment. The latest PowerEdge 12th generation servers can run up to 50% more virtual machines than previous generations and with Intel Xeon processor technology, servers from multiple generations can be combined into the same virtualised server pool to extend failover, load balancing, and disaster recovery capabilities.

Dell DVS Enterprise delivers additional benefits including:

- **Cost effectiveness:** Hospitals are now able to start VDI pilot projects (50-500 seats) themselves using Dell (new or existing) hardware or their own existing non-Dell storage or networking hardware units. The Blueprint, as well as HA feature, are now optional for less than 500 seats, which allows significant savings in the trial phase. If the pilot proves positive, they can expand from there to several thousand virtual seats while using most of the hardware purchased or used in the initial investment phase (no rip and replace).

- **Flexibility:** DVS Enterprise is now qualified on more and the latest Dell hardware (12G Dell servers, and a choice between PowerConnect and Force10 networking switches), with a solution stack that will also work on non-Dell storage and networking units. This allows organisations to use existing qualified hardware to implement a robust VDI solution.

- **Scalability:** As a customer expands the number of virtual desktops, DVS Enterprise scales seamlessly with the addition of new hardware, while still using the hardware purchase previously. This helps reduce the future cost of ownership of the infrastructure from 50 users to thousands of users. In addition, Dell modular, use-only-what-you-need services portfolio can be designed to fit any size installation. Dell philosophy is to partner with healthcare organisations to provide the right assistance based on their needs, skills and resources.

- **Performance:** The use of the latest generation of hardware (servers, storage, networking) ensures access to the fastest CPUs, higher memory configurations, lowest power consumptions, and fastest networking solutions for use of the solution during several years to come. Use of the newest hardware, along with the elements on the core SCL (tested and recommended by Dell) allows optimal performance and decreases the price per virtual desktop. The integration of the latest versions of VMware virtualisation software ensures that the user will benefit from the latest development and optimisation.

VMware View 5.1

- **VMware View** is a desktop virtualisation solution that delivers virtual desktops, applications, and data from the datacentre. VMware View provides a highly scalable administrative interface that improves management and speeds up desktop provisioning. The solution provides increased control and security of the desktop environment through enhanced role-based administration and centralised desktop security policies.

- **vCenter Server** centrally manages VMware vSphere server virtualisation environments, allowing IT administrators dramatically improved control over the virtual environment compared to level of control offered by other management platforms.

- **View Connection Server** is a brokering solution that communicates with vCenter in order to provide management of virtual desktops. This solution includes virtual desktop creation, pool management, and power operations, such as automatic suspend and resume. It may be deployed in an active/passive configuration for redundancy.

- **View Composer** is a software service installed on the vCenter server that provides image management and rapid deployment of multiple link-cloned desktops from a single centralised base image, significantly reducing storage needs while maintaining user settings.

- **VMware ThinApp** provides application virtualisation by abstracting applications from the underlying operating system. The applications are then packaged into single executable files that run completely isolated from one another and from the operating system for conflict-free execution on end-point devices. ThinApp application packages can also be deployed to different Windows platforms.

- **VMware Security Server** offers secure access to View Connection server and allows users to access the virtualised desktop pool from the Internet.

- **View Persona Management** (View Premier edition only) dynamically associates a user persona to stateless floating desktops. IT administrators can streamline migration from physical to stateless virtual desktops while preserving user settings.

- **View Storage Accelerator** optimises storage load by caching common image blocks when reading virtual desktop images to decrease storage load during boot storms.

- **View Enhanced USB** no longer requires a device driver to be installed on the client side. A generic USB arbitrator is implemented on the client side, while a proper USB hub is implemented in the agent. This allows VMware View to support a much broader range of USB devices while supporting fine-grained remote device policy (e.g. enable/disable mass storage file copy) even on multi-function USB devices.

Clients/Endpoints

Health care environments require endpoint devices that always deliver. Dell Wyse thin clients have no moving parts such as disk drives to break down. And with a life span that is typically more than twice as long as traditional PCs, they reduce equipment costs and eliminate refresh cycles. Additionally, centralised management ensures optimal system performance since updates and patches can be performed remotely in minutes and by fewer IT staffers than previously required to service legacy endpoint devices.

Access scenarios for Dell Wyse thin and zero clients include:

- In the ER, a patient has an atypical reaction to anaesthesia. The surgeon pulls up the patient's medical records in seconds to check for allergies and alternative treatment options.
- A clinician verifies a prescription order before dispensing a drug for administration, eliminating a call to the patient's physician.
- While in a patient's room, a nurse checks the pain medication schedule and lets the patient know when the next dose will be given, without having to walk back to the nurse's station.
- A physician signs onto his or her Dell Wyse cloud client via PocketCloud Remote Desktop software to check a patient's chart before responding to an after-hours inquiry.

With Dell Wyse thin and zero clients, caregivers' familiar personalised desktop data and applications are delivered in seconds at sign-on. One end point can run multiple discrete, completely secure sessions successively, with little risk of exposing data. And with support for integrated single sign-on strong authentication, users can log on to their secure, personalised desktop environment in seconds with just a proximity card reader. MCC solution endpoints are required to run a local agent within the device operating system. Supported operating systems include 32 and 64bit versions of Windows 7 on Dell Latitude laptops and Dell Optiplex desktops, WES7 (Windows 7) embedded on Dell Wyse thin and zero clients with Teradici firmware version 3.5 or later. Endpoints may be configured to allow users to log on locally to the device, however, the OneSign agent still requires all configured authentication policy requirements to be satisfied. The client agent is also installed on the virtual machine parent images.

The table below lists the Dell client product families and the features available to each in an MCC environment.

Table 2: Client/Endpoint MCC features

Device Family	Type	OS	SSO	Badge	SWA*	Fingerprint	Multi Factor
Dell Optiplex	Desktop	Win7	✓	✓	✓	✓	✓
Dell Latitude	Laptop	Win7	✓	✓	✓	✓	✓
Dell Wyse P20/P25	Zero Client	n/a	✓	✓			✓
Dell Wyse Z90x	Thin Client	WES7 or WES 2009	✓	✓	✓	✓	✓
Dell Wyse C90x	Thin Client	WES7 or WES 2009	✓	✓	✓	✓	✓
Dell Wyse R90x	Thin Client	WES7 or WES 2009	✓	✓	✓	✓	✓
Dell Wyse X90x	Thin Laptop	WES7	✓	✓	✓	✓	✓
Dell FX100	Zero Client	n/a	✓	✓			✓

*Secure Walk-Away.

Dell Wyse Zero Client Devices

The Dell Wyse P20 (and P25, coming soon) zero clients may be used as proximity card enabled endpoints in MCC View/OneSign implementations. Proximity card-based authentication was first introduced in Teradici firmware v. 3.5 in December 2011. Today, the Dell Wyse P20 ships with firmware v. 4.0 and is fully supported on View/OneSign environments. This version of firmware allows the P20 to communicate with the OneSign appliance and secure the device by preceding normal domain and/or device credential prompts with the OneSign logon dialog. The allowable authentication modalities are user name/password, proximity card and/or PIN, to include any combination for multi-factor authentication to the environment and applications.

Although all supported Dell client devices for MCC provide a rich user experience, performance of Dell Wyse P20 zero clients in the MCC View/OneSign configuration is unparalleled. Initial logon and session transfer times average five seconds in VMware View desktop groups bound to either RDP or PCoIP protocols. The Dell Wyse P20 also dramatically reduces the time and expense of securing and maintaining traditional desktops with centralised provisioning, updates, patches and management. The Dell Wyse P20 provides anywhere, anytime access to personalised desktops from compact endpoints that are easy to mount behind displays, at nursing stations, in patient rooms, or the ER, as well as wireless models ideal for roaming EMR and workstation access. Finally, P20 zero clients also consume very little energy – about 90% less than traditional PCs – potentially saving medical organisations thousands of dollars per year in energy and HVAC (heating, ventilation, and air conditioning) costs. Its low power consumption, small footprint, minimal attack surface, performance characteristics, and comprehensive centralised management using Wyse Device Manager make the Dell Wyse P20 a superb selection for any clinical environment.

The Dell Wyse P20 zero client is the market-leading desktop virtualisation platform for VMware View 5 that incorporates Imprivata OneSign Virtual Desktop Access™ and Teradici PCoIP firmware v. 3.5 to provide a true PC experience with strong authentication.

The Dell Wyse P20 Zero Client

Dell Wyse zero clients facilitate electronic record-keeping in support of strict compliance mandates and ensure faster, more reliable access to critical information and life-impacting applications. With Imprivata OneSign Virtual Desktop Access, caregivers tap a proximity card to an authentication reader connected to the Dell Wyse P20. Within seconds, a personalised desktop session resumes – no sign-in needed.

Other benefits of the Dell Wyse P20 include:

Simple: Secure sign-on takes just six seconds using a proximity card.

Extremely fast: Rapid delivery of rich roaming desktops with all user data and applications.

Ultra secure: No risk of theft, tampering or loss. Centralised management of all applications and data reduces operating and maintenance costs and enables policy-based access control.

Cost-effective: Scalable deployment reduces CAPEX for growing organisations; low power consumption – up to 90% less than PCs – minimises power and cooling.

Performance: High-performance and brilliant graphics processing.

Well-connected: Easy connectivity via Ethernet over LAN or WAN with 4 USB ports to attach a variety of peripherals, including proximity card readers.

Easy-to-manage: Central management to increase security and simplify provisioning, maintenance and updates

Green: Uses less than 15.5 watts of power in full operation

Rich user experience: Multiple display support with multimedia playback and HD audio

Dell Wyse P25 Zero Client

The Dell Wyse P25 next generation zero client may also be used as a proximity card endpoints in MCC View/OneSign implementations. The zero client uses the latest Tera 2 PCoIP processor from Teradici coupled with client-side caching to optimize available network bandwidth. It has the ability to support two HD displays if needed and draws significantly less power than the P20 consuming less than 8 watts when the P25 is connected to one keyboard, mouse and monitor. The form factor is also a lot smaller which makes it easy to mount it to the rear of a monitor.

One important thing to note when using the P25 in a MCC View / OneSign environment is to make that the screen resolution of the monitor matches the screen resolution on the virtual machine. (If they do note match, the virtual machine will not be visible).

Imprivata OneSign 4.6

Imprivata OneSign provides secure authentication and application single sign-on (SSO) that removes the need for doctors and nurses to remember and type multiple passwords; reducing login time and helping hospitals achieve, maintain, and streamline compliance. OneSign also extends identity-centric authentication and access services across system and geographic boundaries with completely distributed management, delegated administration, and business continuity capabilities. OneSign's integrated authentication management, single sign-on, remote access and functionalities allow healthcare organisations to successfully establish a single centralised employee IT access policy for every aspect of access across all users, rights, locations and conditions.

- **OneSign Server Appliance** is a purpose-built physical or virtual appliance that is highly secure, and requires no changes to the organisation's existing IT infrastructure, including the AD schema. The physical appliance is a 1U appliance. Two appliances are provided enabling built-in redundancy and automatic hot failover if necessary. The Appliance manages user passwords, user profiles, application profiles, and authentication modalities. In customer environments where proximity badges are already in use for building access, existing badges may in some cases be also be leveraged for MCC authentication.

- **OneSign Agent** resides on client-side workstations and virtual desktops to manage user access and upload user activity data to the OneSign Appliance. In a zero client environment, OneSign Agent is integrated with the device firmware. The Agent handles authentication of users locally through ID badges, fingerprint biometrics, or one-time tokens and passwords. Once a user authenticates to the OneSign system, the user may be automatically signed in to deployed applications as they are launched. The OneSign Agent handles the local transaction of proxying user credentials to applications and domains. The OneSign Agent downloads credential and application information from the OneSign Appliance at login, and queries for changes at an interval determined by the OneSign Administrator. The agents will "heartbeat" the appliance and automatically switch to the hot-standby appliance if connectivity is lost from the primary appliance.

- **OneSign Administrator UI** is a web-based interface for managing all aspects of the OneSign configuration including users, applications, agent settings, password automation and audit reporting.

- **Single Sign-On (SSO)**: Provides increased security by sending single-use authentication credentials. SSO allows for increased security for users who have access to sensitive data. Applications requiring credentials for access are profiled within the SSO solution. Once the application profile is generated, users are only prompted once for credentials for that application. At first logon at the start of each worker's shift, the credentials are stored with his or her user profile. Subsequent logons do not prompt user for credentials and are automatically submitted for the user streamlining the authentication process. Policy may be set to allow users to manage their passwords, but the user convenience and added security of advanced authentication with SSO using badges/card and/or biometric authentication makes that option much less relevant.

- **Session roaming**: Reduces the risk of unwanted password sharing or the creation of "generic" user accounts for application access by roaming users. Enabling a user-specific corporate workspace from multiple shared MCC clients reduces or eliminates the risk of password sharing; users now have means for creating individualised OS environments and applications per session on any system. To increase the speed of session roaming, the session remains active, although in a static state until complete log off by the end user occurs. While in the static state, it can quickly be directed to any enabled endpoint within the enterprise.

- **Role-based Access**: Users can only see the applications provided per Role Based Access definitions; thereby limiting application access to appropriate users. IT departments can implement comprehensive policies to allow or deny access based on an employee's status, role, badge events and/or physical location. User profiles are generated within the SSO solution and linked to user's logon credentials. You may also use profiles to specify which image is used to generate the user's virtual desktop. For example, physicians and nurses may receive a Windows 7 based desktop, while technicians receive a Windows XP based desktop.

- **Security Server/ Gateway**: For remote users, encrypted points of access from the Internet to the data center servers using SSL (HTTPS).

    1. Transparently encrypts and authenticates all connections to protect against potential threats;
    2. Denies direct access to internal corporate resources from the Internet;
    3. Can use two-factor authentication without touching servers;
    4. Provides a simplified client firewall;

- **Secure Endpoint Access**: Security software for SSO and strong authentication is distributed to end-user devices, but centrally managed in the datacenter. Agents loaded on the endpoints check in with the SSO solution for updates and/or changes in the security policy at an interval determined by the system administrator. You can set the interval as frequently as needed. Multiple security profiles may be defined with different levels of required authentication. For example, a biometrics/fingerprint scan may be combined with smartcard or PIN for multifactor authentication where higher level security requirements exist.

- **Authentication:** Authentication options are set in the OneSign administrator's management console and applied to users based on existing directory group memberships, globally, or individually. When a new authentication policy is applied, users can self-enroll their cards or fingerprints, simplifying roll-out and decreasing administrative overhead. OneSign also supports supervised or managed enrollment. To be considered true multi-factor authentication, authentication policy should require at least one form of authentication from at least two categories of authentication. Common multi-factor combinations are Proximity Card + PIN or Fingerprint + PIN. The Dell MCC solution allows for multiple combinations of authentication to meet both compliace and hospital security requirements, including:

    1. Coded passwords, such as password or PIN;
    2. Physical tokens such as a card, badge, token, or device;
    3. Biometric physical authentication using fingerprint

- **Secure Walk-Away™**: Secures desktops from unauthorised access to confidential information assets by automatically securing desktops when a user departs from their workstations. Secure Walk-Away (SWA) utilises facial recognition and motion detection in order to trigger a session lock event. End points, equipped with a supported web camera, automatically create a digital key from the user's facial features. When the user moves away, the desktop is automatically locked. When the same user returns, they are recognised and the desktop is automatically unlocked. No images of the user are captured or stored and no images are sent to or stored on the OneSign Appliance. SWA may be customised per customer requirements. The duration to obscure, lock the desktop, and assign a grace period to return to the desktop for facial recognition authentication may all be tuned to customer needs. SWA requires an onboard or USB-attached webcam to perform facial recognition. For enhanced security, policy may be set to lock the endpoint session if the external webcam is unplugged.

- **OneSign Self-Service Password Management:** This feature provides a portal that a user can access instead of calling the helpdesk to reset their primary domain password. It can also be used by non-network users such as contractors to request a OneSign directory account.' as well as 'OneSign Physical/Logical which integrates with leading building access systems such as those from AMAG, Honeywell, Lenel, S2, and Tyco allowing additional control over the authentication process. As an example, Imprivata OneSign Physical/Logical can confirm as part of the authentication chain, that a user has legitimately entered the building by presenting their smartcard at a door access system sensor before allowing them to complete their computer authentication. This can be used to prevent tailgating and ensuring that only authorized individuals can access company systems thereby providing a complete location aware solution for access and authentication'

- **Centralised Security Policy for Users and Groups:** Controls user authentication methods, lockout rules for authentication violations, user challenges, user session concurrency, hot-key locking of shared workstations, and sets the rules for password self-services. A user can be locked out after attempting to access his account in violation of the rules set in the user's security policy.

- **Secured Communication:** All agent to appliance communications are routed through secured SSL channel/ HTTP(s) port 443 or 81 and AES 128-bit encryption. Appliance to appliance communications and database replication are sent over encrypted tunnels on ports 22 and 1521 using the proprietary Imprivata Secure Exchange (ISX) protocol.

Disaster Control/Recovery and High Availability

Digitised medical records can reduce medical errors, improve patient safety and produce better clinical outcomes—but if the caregivers cannot access a crticial application like EMR because their datacenter is down, the consequences can be serious. When electronic devices replace paper charts and physician prescription pads, the reliability, availability and security of the underlying system delivering clinical workspaces becomes critical. That is why modernisation of the point-of-care desktop has become an urgent priority for hospital IT professionals as well as hospital caregivers. Desktops and patient care applications must be immediately accessible and available to clinicians and nurses even in the event of site failures and outages. With Dell MCC VMware View Solution, healthcare organisations can now have unparalleled desktop and application reliability and availability.

The Dell MCC VMware View Solution centralises each user's application or desktop in the datacenter. You can generically deploy the corporate client system with limited applications installed locally or with applications delivered from the data center. In cases of disaster, this deployment translates into client systems being redeployed from generic images, which enables a faster recovery time to a fully operational state.

The Dell MCC VMware View Solution can also be set up in a High Availability and scalable server cluster environment to eliminate single points of failure and to support any planned or unplanned system downtime in the daily hospital routine. The High Availability environment includes setting up the servers up in a Network Load Balancing server cluster and in a High Availability configuration. The SQL database server is configured in an active-passive mode one is the active node and the second has an instance of the database that is passive to ensure operational continuity and minimise downtime. When deployed in a cluster, native DRS, HA and vMotion are enabled for increased redundancy, fault tolerance and uptime. The View Connection server role may also be deployed across multiple nodes. Backend storage for all server components is configured in RAID 5, RAID 6, or RAID 10 (per customer requirements) with multiple interfaces and paths configured for network redundancy.

In environments requiring redundancy and fault tolerance at the virtual desktop level, Dell offers the **VMware AlwaysOn Desktop** reference architecture that allows clinicians and staff to achieve the continuous level of availability they demand. Beyond the redundancy of backend servers and infrastructure, this configuration allows for multi-site and multi-instance replicas of the entire VDI environment, able to sustain site failures with automated roll-over to standby sites and infrastructure. By having an Active-Active desktop environment running identical desktop images, even if there is a failure at the primary site, end users can promptly access their desktops and applications. If a healthcare provider's infrastructure is compromised through a natural disaster or other outage, clinicians—who are many times among the first responders—can be assured they can reach their clinical desktops and applications where and when they are needed the most.

This new architectural design features continuous monitoring capabilities, as well as load balancing with constant data replication across sites to ensure that if the primary site is down VMware AlwaysOn Point of Care Solution will seamlessly AlwaysOn Point of Care Solution will seamlessly route the end user to the secondary site so the clinician experiences minimal disruption. As a result, IT can now deliver non-stop point of care desktops with all applications and data readily available where and when they are needed most.

Security

In healthcare IT environments where fast access to clinical applications and data is critical, in the interests of saving time, many clinicians and nurses practice poor data security by using overly simple and even shared passwords, thereby increasing the risk of data breaches and data incursions. In addition, caregivers today increasingly use sophisticated tablet devices and smartphones in the workplace to save time and streamline their workflow.

Desktop infrastructure is especially vulnerable. Human error, email attacks, network-borne viruses and malware, infected websites and downloads put data at risk every day – potentially on every traditional desktop. The ongoing consumerisation of

IT has healthcare organisations struggling to protect sensitive data and corporate assets, while maintaining acceptable network performance and user experience. Security breaches mean healthcare providers can potentially incur steep fines for sensitive data that is sent to the wrong printer, data incursions, or lost mobile devices such as smartphones and tablets that contain patient data in violation of security protocols.

Common security pain points in healthcare environments include:

- Endpoint vulnerability due to malware, viruses, theft, loss and hardware failure.
- Data vulnerability due to unauthorized access and removal of data via removable USB media
- Difficulty of securing hundreds or thousands of PCs with the most recent patches and updates to consistently meet compliance requirements.
- A proliferation of new tablets, smartphones and laptops introduced to the network as a result of workplace trends such as consumerisation.
- The time and effort required to add single sign-on or two-factor user authentication to individual PCs in highly secure locations.

Many organisations are looking to desktop virtualisation as an effective solution; virtual desktop infrastructure (VDI) is less vulnerable because data resides in a secure datacenter rather than on vulnerable endpoint devices and strict security and access policies are easily applied and managed from a central location. Compliance with government and/or industry-mandated regulations is also much easier with VDI architectures, because IT maintains complete visibility and control over network and file access, data storage, and system maintenance.

To address many of the common security pain points, Dell MCC VMware View Solution leverages application and desktop virtualisation technology to deliver users' operating systems, applications, and data. Resource centralisation reduces data security risk from user endpoints via theft or mismanagement, and improves business continuity by providing greater consistency to distributed data, and applications. Centralisation also allows end-user access via role-based access profiles, including centralised changes being propagated per user vs. client end-point.

The solution allows administrators to set policies that make access conditional based on location, network and user type, thereby reducing the potential for data loss and providing better manageability and disaster recovery at the enterprise level, because the data does not reside on the local client – only encrypted screen data is pushed to the endpoint device. In addition, the solution allows administrators to proactively manage security threats centrally in a data center as opposed to on every device, providing cost savings and increased availability for end users.

With Imprivata OneSign, Dell MCC VMware View Solution adds an enhanced security layer for healthcare organisations. Security is built in the architecture of OneSign through Secure Endpoint Access, Security Server/ Gateway, and Secure Communication functionalities. From an end user standpoint, OneSign features including Multi-factor Authentication, Secure Walk-Away, Centralised Users and Group Policies and Role-based Access minimise the need for caregivers to remember and type multiple passwords while allowing hospitals achieve, maintain, and streamline compliance. Imprivata OneSign allows healthcare organisations to successfully establish a single centralised employee IT access policy for every aspect of access across all users, rights, locations and conditions.

From a client device standpoint, Dell Wyse thin clients provide an added element of security since all data resides on servers in the data center, simplifying regulatory compliance and disaster recovery. End points can be locked down through centralised management and authentication solutions, and highly secure mobile access to crucial patient data can be achieved in seconds with integrated single sign-on strong authentication solutions. Finally, Dell Wyse zero clients that are purpose-built for VMware environments have no data or OS running locally and no attack surface, and are therefore less likely to be affected by viruses, malware, theft or data loss.

Dell Wyse thin and zero clients are ideal for environments that require high security and reliability. With Dell Wyse clients, IT staff can customise policies to define the performance, security and functionality profile of a virtual desktop for any user,

from mobile workers to power users to support staff, and adapt to various business initiatives, including off-shoring, mergers and acquisitions, and branch expansion. With an open, scalable and proven architecture, Dell Wyse simplifies management, support and integration, while providing a completely secure, reliable computing platform that meets even the most rigorous security and compliance requirements. Healthcare IT departments will appreciate including:

- Centralises network management for complete visibility and control over end user device access and use, regardless of the access device or location.
- Enables rapid, cost-effective and consistent updates and patches to ensure device security and software image and application consistency.
- Simplifies policy administration for consistent compliance with various industry and governmental regulations.
- Enables easy and timely integration with a variety of single sign-on, strong authentication devices for enhanced security when necessary.
- Significantly reduces the threat of data loss through malware, viruses, or theft of hardware failure, because all data and applications are stored in the secure datacenter – where it belongs.

System Management

Systems management functions are provided through vCenter, View Manager, OneSign SSO administrative interface, Wyse Device manager, and the Teradici PCoIP Management Console. For systems management needs above and beyond those native to vSphere, View and SSO provider, refer to standard Dell or Enterprise systems management technologies at the link below.

DVS Enterprise streamlines OS migrations, application updates, and security patches by relocating the OS, applications, and user settings from client systems to the data center for centralised desktop management. Administrators can avoid making time-consuming desk-side support visits to resolve software-related issues. For example, locked master images enable 'self-healing' – when users encounter system issues, the IT department can simply reboot and restore a clean image. Dell DVS Enterprise delivers a simple, reliable and complete way of using centralised desktop management to provide users with secure access to data and applications enhancing flexibility, leveraging consumerisation and BYOD trends, and ultimately optimising productivity.

The Dell MCC solution allows IT departments in healthcare environments to easily manage thin and zero clients throughout their enterprise, regardless of their deployment location. Dell Wyse Device Manager (WDM) software enables easy configuration, insight, and management of anywhere from a handful to several thousand Dell Wyse endpoint devices. Dell Wyse WDM provides secure HTTPS-based communications and a powerful device policy for configuration management. The solution enables real-time asset management and health monitoring based on an industry-standard SQL database and optimises remote software repositories.

Among the features the Dell Wyse Device Manager (WDM) provides are:

- Secure HTTPS based communications.
- Powerful device policy and configuration management.
- Real-time asset management and health-monitoring based on industry-standard SQL database.
- Remote imaging.
- Optimisation of remote software repositories.
- Administration delegation for third party support staff.
- Common Criteria certification.

Dell MCC Consulting & Implementation Services

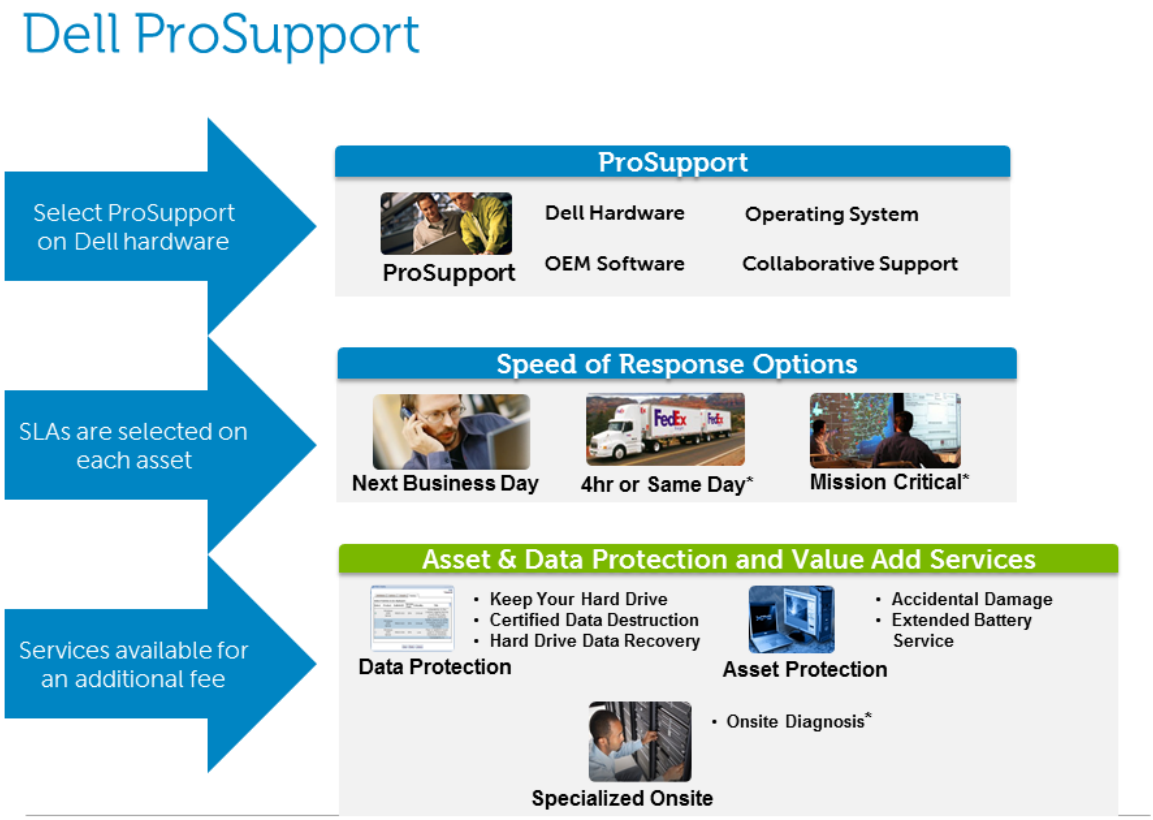
The Dell MCC Consulting Services team provides Discovery, Blueprint, and Design services to design the optimal reference architecture based on a holistic understanding of a customer's requirements, computing environment and clinical workflows. Dell MCC solution experts work with hospitals to understand their specific business needs, requirements, and constraints through onsite Discovery workshops. Dell experts also help hospitals map a transformational Blueprint from 'As-Is' state to 'To-Be' state through Blueprint assessment; then create a robust and scalable design to define detailed hardware and software requirements and services scope of work. Dell's Discovery, Blueprint, and Design services will help healthcare organisations identify how to maximise the benefits from the MCC solution.

Dell MCC Implementation Services teams are responsible for project management and end-to-end integration services including desktop virtualisation, application virtualisation, identity access management, data center installation and configuration, client deployment, and other services. Dell MCC services teams group can deploy a 50-500 user production pilot to allow healthcare organisations to experience the flexibility and enhanced productivity benefits that the solution delivers. And when hospitals are ready to roll out the solution, Dell services teams will be there to help design and implement a scalable solution that delivers the benefits of Dell's MCC solution to thousands of users across multiple sites. .

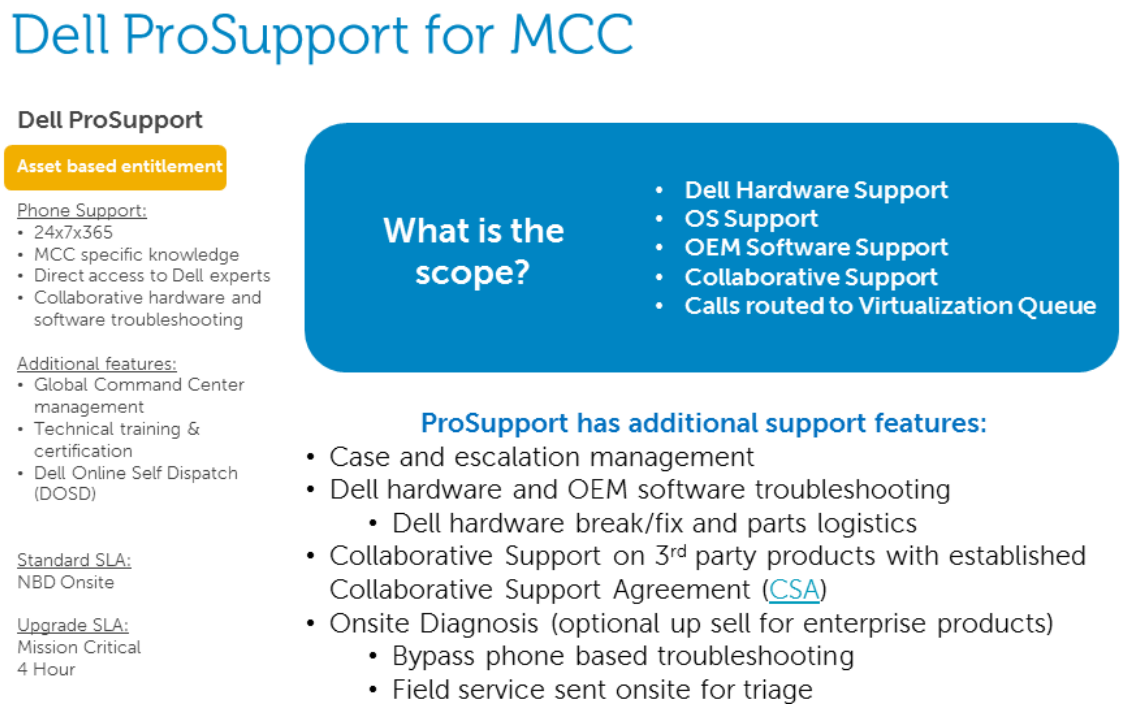
Dell ProSupport

Dell ProSupport is a portfolio of premium hardware, software and solutions support services available 24x7x365, globally. Dell ProSupport services enable hospitals to simplify their internal support processes; and fill gaps in their IT support resources, expertise, and coverage to ensure uptime and meet user demands, while providing a single source of accountability through collaborative support coordination across multiple vendors with escalation management.

- Single point of accountability with highly-trained experts.
- Next Business Day onsite service with four and eight hour parts and labour response options.
- Third-party collaborative assistance for hardware and software issues leveraging Dell's relationships with leading software vendors.
- Escalation management with customer-set severity level options.
- Solution support expertise in specialised applications and software, including desktop virtualisation software included in the solution.
- Access to Dell's centralised global command center that tracks and provides status updates regarding ProSupport technicians' availability and replacement part ETA, around the clock.



Dell ProSupport MCC solution helpdesk and field support technicians are highly-trained specialists who are knowledgeable of every component of the lab validated MCC solution configurations including enterprise hardware and software technology, endpoint devices, desktop virtualisation software, and identity access management software. These technicians are certified in VMware vSphere & View, Imprivata, and Wyse technology and receive ongoing training.



References

Dell Mobile Clinical Computing Solution
http://www.dell.co.uk/MCC

Dell Mobile Clinical Computing Solution BVIT trials proven results information and whitepaper
http://www.dell.co.uk/provenresults
and
http://www.dell.com/Learn/uk/en/rc1050265/healthcare/mcc-landing-whitepaper-uk?c=uk&l=en&s=biz&cs=RC1050265

DVS Enterprise Reference Architecture: Mobile Clinical Computing
http://go.us.dell.com/dvsmcc

Appendix 1.0

Proximity Card Examples used in each region:

UK, France, Germany, Netherlands

Readers: MiFare reader such as the RFIDeas External USB reader, OMNIKEY® 5321 CR USB Reader, Gemalto ProxDU reader
Proximity Cards: Compliant Protocols: HID® iCLASS® and MIFARE®, as well as ISO 14443 A/B and ISO 15693

Smart Card Examples used in each region:
Below, find examples of cards used in each country to date:

UK
Smart card: NHS V5 Smart card
Readers: Contacted Smartcard reader in the Dell Keyboard, MiFare reader example RFIDeas External USB reader

France
Smart card: CPSV3 card (combination of proximity card and smart card)
Readers: Gemalto GemPC Smart Card Reader for smart card authentication. For proximity authentication, use Omnikey 5321 reader or the Gemalto ProxDU reader.

Germany
Readers: OMNIKEY® 5321 Desktop USB Reader
Cards - Compliant Protocols: Supports HID® iCLASS® and MIFARE®, as well as ISO 14443 A/B and ISO 15693

Netherlands
Readers: OMNIKEY 3121 USB Card Reader
Card Type – UZI-pas


CPS
CARTE DE PROFESSIONNEL DE SANTÉ
ORDRE NATIONAL DES SAGES-FEMMES
SAGE-FEMME
0 0B5004565
Mlle SAGE-CH0456 CELINE
2300071298
expire fin 03/2014
TEST
Testkarte HBA G1
STARCOS 3.4
Version 2.3.2
Giesecke & Devrient
25.07.2011
NHS Care Records Service
445229014045
IT Test One


Cette carte est strictement personnelle.
Toute personne trouvant cette carte
est priée de bien vouloir l'envoyer
sous pli non affranchi à :
asipsanté
ASIP Santé
Libre réponse 31967
75742 Paris Cedex 15
esante.gouv.fr
Signature du porteur
Warning!
This test version is intended exclusively for test purposes in test environments. Using this test version outside a test environment might cause damage. As governed by law, G&D is not liable for any damage resulting from using this test version in another way than described above.
Giesecke & Devrient
Creating Confidence.
This card is the property of the NHS.
If found, please post free to:
Freepost, PO Box 621, Leeds, LS1 4WD.
0501302341