



## White Paper on Security

Written by: Michael Arner, Chief Technology Officer

# Table of Contents

<b>1.0 Introduction</b>	<b>3</b>
1.01 ROAM Data Security Architecture Overview	3
<b>2.0 Transport-layer Security</b>	<b>4</b>
2.01 Encryption	4
2.02 Protection Against Client-side Tampering	4
2.03 Protection Against Middle-man Attacks	4
<b>3.0 Application-layer Security</b>	<b>5</b>
3.01 Back-end Authentication	5
3.02 Control Center Entitlement	5
<b>4.0 Payment Security</b>	<b>5</b>
<b>5.0 Security Between ROAM and the Enterprise's Corporate Systems</b>	<b>6</b>
<b>6.0 Protection Against Device Loss or Theft</b>	<b>6</b>
6.01 Persisted Data	6
6.02 Unauthorized Application Use	7
<b>7.0 Operational Security</b>	<b>7</b>
7.01 Username Requirements	7
7.02 Password Requirements	7
7.03 Required Password Change	8
7.04 Invalid logins	8
7.05 Inactive Accounts	9
7.06 IP Address Blocking	9
7.07 Preventing Robotic Access	9
<b>8.0 Conclusion</b>	<b>9</b>

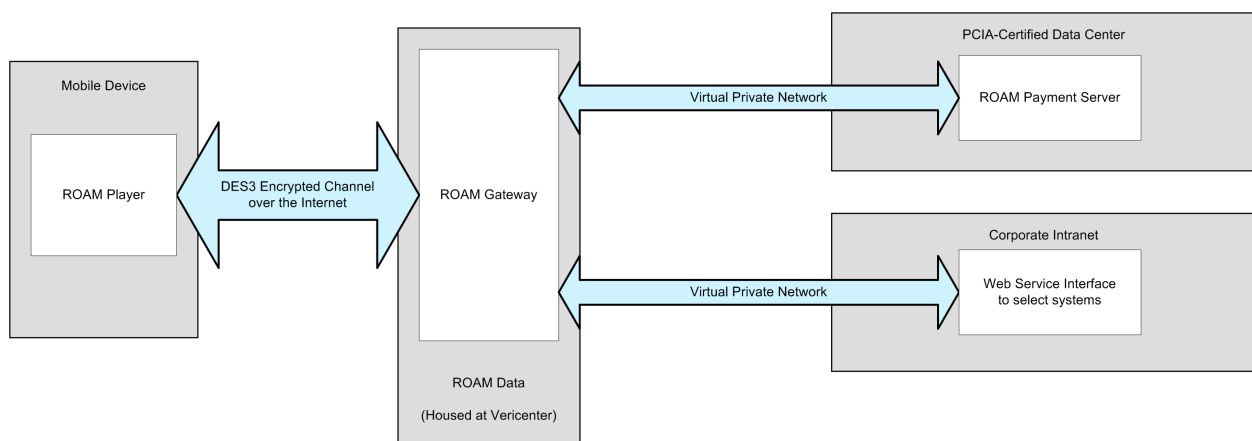
# 1.0 Introduction

To properly enable Enterprise Mobile Applications one must be able to adequately answer the Enterprise's security concerns: How to safely connect valuable corporate data and corporate functionality across a public Internet to a fleet of devices which may easily be lost or stolen? How to ensure unauthorized personnel do not gain access to corporate data? How to ensure sensitive information, including payment related information, is not exposed to potential criminals from the device, all the way to the intended destinations.

The ROAM Data solution has been architected from the ground up with these concerns in mind: to provide end-to-end security for the enterprise; to meet and exceed the rigorous requirements for PCI (Payment Card Industry) certification; and to render compromised devices innocuous. ROAM's solution replaces the web-browser (which may be redirected to malicious URLs) with a Smart Client ROAM Player that is only capable of connecting to a single, dedicated secure ROAM Gateway Server. The Gateway Server itself is not a traditional web-server, but an authenticating, auditing, and highly-secure proxy server, intermediate between the device and the enterprises' Corporate Systems. These Corporate Systems remain entirely unexposed to the public web.

This white paper provides an overview of the security components of the ROAM Data architecture.

## 1.01 ROAM Data Security Architecture Overview



## 2.0 Transport-layer Security

### 2.01 Encryption

The ROAM Player communicates with the single ROAM Gateway for which it has been provisioned via a channel encrypted using the Payment Industry standard of Triple DES (DES3) algorithm and a 196-bit key across http, the same mechanism used by the well known protocol, Secure Socket Layer or SSL. The ROAM transport layer differs from SSL in that the latter allows anonymous authentication via an exchange of keys using the private/public key algorithm, RSA. The ROAM architecture permits no anonymous authentication. The player submits credentials unique to its individual provisioning, so that the server can immediately identify player/ device/user and employ an encryption key unique and specific to that provisioning.

DES3 with 196-bit key, as the standard for the Payment Industry, is ROAM's default mechanism for transport-level security. If required, ROAM can also support encryption using the AES algorithm. If desired, ROAM has the option of also increasing key sizes for additional security (at a slight cost in performance speed).

### 2.02 Protection Against Client-side Tampering

Individual player credentials are stored in a settings file on the device which has been encrypted using a separate DES3 key internal to the player executable and hashed using the SHA-256 algorithm to protect tampering. Detection of a modified settings file causes the ROAM Player to shut down.

### 2.03 Protection Against Middle-man Attacks

Communication between the Player and the Gateway is also hashed using SHA-256 and a seed created with user credentials AND the player system time-stamp. Any tampering with a packet between Player and Gateway will cause the message to present a bad hash and will cause the session to drop until re-authentication. Any re-submission by malicious intermediaries of a previously submitted package will fail server-side restrictions on valid time-stamps (i.e. time-stamp must increase from message to message and must represent a reasonable delta from the previous message).

## 3.0 Application-layer Security

### 3.01 Back-end Authentication

One of the web-services the Enterprise back-end will employ is an authentication mechanism of its own, verifying username/password credentials that are specific to the distributor, consultant, employee or IBO and that are unknown to ROAM Data. These credentials are submitted via a login screen as the first screen (and first web-service call) of the application.

### 3.02 Control Center Entitlement

In addition, the ROAM Gateway matches configurable entitlements between a user and an application (or even between a user and particular web-service call within that application) with every call. These entitlements are set via a Control Center securely hosted internally at ROAM Data. During the registration process for each end-user, their identity is verified and reference cross checked against their Enterprise username/password; then the specific rights for the allowed application(s) are registered for that user. The end-user will only have access to the application and information he/she is entitled to have.

The two application-layer security mechanisms — one at the enterprise and one at ROAM — allow either agency to deny any user access to any application or to any portion of any application whenever deemed necessary. A device reported lost or stolen, for example; or an employee terminated; or activity that is flagged as unusual, may be selectively shut out of the system (or restored into it) at a moment's notice.

## 4.0 Payment Security

Besides transport-level security, information tagged as "payment information" is encrypted by the player a second time (i.e. in addition to the default transport-layer encryption) using a separate, second, 196-bit Triple DES Key which is also unique to the provisioned device. This information never exists in plaintext on the ROAM Gateway (which does not store the second key but only submits it to the payment server upon a device provisioning), is not audited (as is the data of every other web-service call), and can only be decrypted by the ROAM Payment Server at a PCI-certified site.

To comply with PCI DSS Certification, ROAM Data maintains rigorous operational procedures from development to deployment, From signoff on code to be deployed, to maintaining production-side security patches at the server and network level. We have a sign-off process in a staging area before deploying to production. ROAM also goes through PABP (now PA DSS) to maintain Payment Area Best Practices. Secure backups are stored off site. All deployment of new software is extensively documented.

Physical security at the data center where the ROAM Payment Server is hosted is fully PCI DSS compliant: including security camera monitoring, access control, the logging of all personnel access, criminal background checks on all personnel requesting access, etc.

## **5.0 Security Between ROAM and the Enterprise's Corporate Systems**

A fundamental goal of the ROAM architecture is that Enterprise functionality not be publicly exposed in any fashion on the Internet. ROAM recommends employing a VPN connection between the ROAM Gateway and the Enterprise back-end, allowing only SSL-encrypted traffic with a single outside IP Address. ROAM applications themselves only have access to the subset of functions the organization encapsulates for the solution via web-service; and back-end authentication (see section 3.1) protects the individual application session against unauthorized use.

## **6.0 Protection Against Device Loss or Theft**

### **6.01 Persisted Data**

By default, no personal data resides on the device.

In an off-line situation, an application is allowed (if the developer decides to do so) to temporarily store encrypted form data on the device using the same DES3 key that encrypts transport data (this form data is then erased with a return online), but under no circumstances is any application data ever stored openly on the device.

## 6.02 Unauthorized Application Use

A lost or stolen device is de facto unable to authenticate against the Enterprise back-end (as the application-level login/password will be unknown to unauthorized users) to begin an application session. In addition, a device reported lost or stolen can be prevented from even pinging the Enterprise back-end by turning off application-entitlement at the ROAM Control Center (see section 3.0).

# 7.0 Operational Security

Operational security encompasses the set of process restrictions and procedures that are not necessarily built into the source code of the system, but that nonetheless affect the user's use of the system.

## 7.01 Username Requirements

ROAM applications typically inherit usernames from the enterprise and thus adhere by definition to the enterprise's username policy. The exception to this is the use, detailed below, of special characters. The user can optionally change their ROAM username to an all-lower-case, all-alpha, no-special-characters version of their enterprise username.

## 7.02 Password Requirements

Applications in the mobile environment need to strike a slightly different balance than desktops when it comes to the types of data input required for authentication. Thus passwords are allowed to be all-alpha-single-case or all-numeric due to the extraordinary contortions mobile users must often go through to switch between alpha and numeric, or upper and lower case, on the mobile device. Requiring special characters renders most devices unusable and is not allowed to be configured. Because of this limitation on password policy based on the limitations of the device, user passwords are, by default, required to be a little longer than is typical, at least 8 characters long, but this can be configured by the enterprise to be longer.

### Passwords may:

- be 8 to 30 characters long
- be 8 to 30 characters long
- be all upper or all lower case

- be all alpha or all numeric

**Passwords may not:**

- contain special characters (including dash and underscore) or spaces
- be a single character repeating
- be the same as username
- contain users first or last name
- be any combination of users first and last name
- be the same as enterprise name
- be sequential numbers
- be any of the users phone numbers
- be a password used by more than MAX\_SHARED\_PASSWORD of other users in the enterprise
- be a word in the enterprise-supplied list of prohibited passwords

## **7.03 Required Password Change**

Passwords can be configured to be change-required on a number-of-days basis. This is not required by default. Required password changes have a configurable number-of-days grace-period.

## **7.04 Invalid logins**

There are two levels of authentication to consider – device level and user level. The device logs in with credentials provided on provisioning each time it connects to the ROAM gateway.

### **Device Level**

At the device level, a new device that fails login is redirected to a site from which the user may obtain a valid provisioning if, and only if, he passes exactly the same authentication mechanism that a new user applying for a provisioning to the generic ROAM system would pass. Thus, from the perspective of the enterprise, a device that fails login (as opposed to a user who fails login) is, by default, divorced from the enterprise until such time as the user successfully navigates the same manual provisioning process as a brand new user.

A device that fails login MAX\_FAILED\_DEVICE\_LOGINS times is shut off permanently and can only be re enabled by manual intervention.

## **User Level**

A user who fails login MAX\_FAILED\_USER\_LOGINS times is, by default, shut off permanently and can only be re-enabled by manual intervention. This behavior can be modified to suit the needs of the enterprise such that, for example, a secret-question/emailed-password mechanism can replace the permanent shutoff.

## **7.05 Inactive Accounts**

ROAM automatically locks accounts that have not logged in to the system for 30 days (configurable). Accounts that have never logged in get an extra 30 days grace period to allow for device delivery, training and other startup issues. A locked account must be unlocked manually through tech support.

## **7.06 IP Address Blocking**

IP addresses geolocated in countries not supported by the enterprise are blocked completely from access to the enterprises hardware on the network. IP addresses geolocated in countries NOT supported by any enterprise in the ROAM system are blocked from access to any portion of the network. An IP address that fails login MAX\_FAILED\_IP\_LOGINS (typically MAX\_FAILED\_USER\_LOGINS times 3) are blocked.

IP addresses may also be blocked at the discretion of operations based on the output of intrusion detection and intrusion prevention systems within the network.

## **7.07 Preventing Robotic Access**

Forms within the desktop web applications which provide access to any secure information in the system, including authentication success/failure are protected by CAPTCHA mechanisms which prevent scraping.

# **8.0 Conclusion**

ROAM Data is committed to the end-to-end security needs of its clients. The architecture is a versatile one which can be adapted to special systems-level or application-level requirements of a particular solution where such are required. Please feel free to contact ROAM Data with any additional questions.