dormakaba

# Keyscan Aurora
## Centrally managed access control

A new age for access control


Brochure

# How to remove end-user barriers to access control and generate a new stream of recurring monthly revenue

The world of Physical Access Control is experiencing a paradigm shift as it relates to value optimization. Integrators that operate central stations are making the leap from burglar or security system monitoring and have begun to apply the same recurring monthly revenue (RMR) model to physical access control solutions.

This progression leverages the expertise and infrastructure of the Central Station Integrator, creating lucrative RMR while offering significant value for the access control customer.

Integrators/Central Stations offering access control as a service are finding that this model dramatically reduces the cost of entry for the access control customer eliminating the need for onsite computers or server equipment required to support the access control system.

Some offer the access control panels as part of a lease or maintenance agreement to further enhance the benefits and reduce the entry level cost of a physical access control system.

This paper discusses the access control as a service model, technology solutions, expansion topologies and how Keyscan products are engineered for recurring monthly revenue.

**Introduction**
With access control and security being required for most companies, large or small, the complexity of supporting such systems combined with the entry cost of implementing an integrated system can be a daunting task.

In some cases, having computer hardware on site and assigning an access control and security administrator is simply not feasible or desired based on the company makeup and staffing levels.

In some cases, a company's sole desire may be to outsource the day-to-day system management and free their time up to focus on the core competencies that drive revenue for the company. This is where the tangible advantages of access control as a service prove extremely enticing and directly explains the significant uptake of companies moving to this model for their access control solution.

After careful consideration and consultations with central stations and integrators, Keyscan has developed a refined solution for a centrally managed access control system without compromising physical or network security and providing extreme fault tolerance and elite capabilities for the end-user.

Overall, access control as a service no longer means end users must compromise or limit their system expectations.

**The internet communication topology**
While internet communications do pose some technology challenges and security threats that must be considered, it proves to be the most cost effective and ubiquitous communication medium today.

Challenges such as navigating through firewalls, anti-virus services and port forwarding in many cases can require a highly trained IT savvy individual for setup and configuration.

This has been the limiting factor for many Integrators and Central Stations that have investigated access control as a service. Although the RMR is enticing, many have not had the necessary in-house technical resources to implement the access control as a service model and have not pursued it further.


At Keyscan we have refined our communication media beyond the typical LAN/WAN application and are introducing internet-based solutions.

Recognizing the market demands and significant opportunity for access control as a service Keyscan has engineered a solution that minimizes the complexities associated with internet-based deployments and lends itself to the access control as a service RMR model.

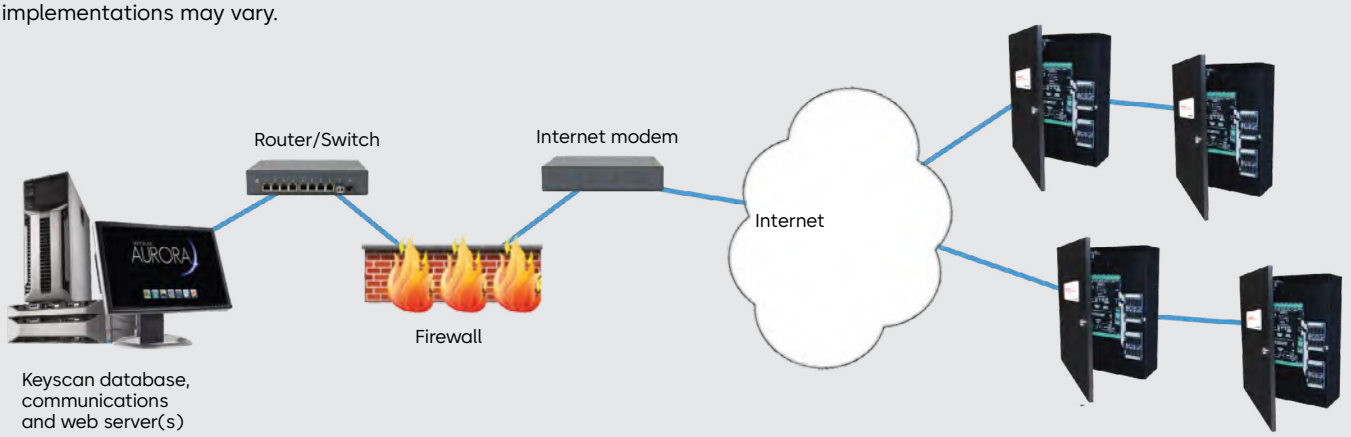
**Data and system security**
Placing a system that's true intent is access control and security on the internet runs counter to most security professionals comfort level and raises some hard questions about system security and susceptibility to internet-based hacking.

Keyscan has addressed this concern by using its NETCOM6P series of Ethernet adapters that include a 256bit AES Rijndael layer of encryption. Both the remote customer site and the host receiver software are deployed with the highest level of data encryption technology.

This level of encryption is approved for TOP SECRET file encryption by the United States government and as such is sanctioned for use only in non-embargoed countries. This encryption provides the ultimate in security and is extremely well suited for panel-initiated internet data transfers.

**System expansion**

Diagram for informational purposes only. Actual implementations may vary.




**System design central host**

Deploying centrally managed access control at the host or central station is as simple as acquiring the necessary server(s). Keyscan's software and database are managed and run at the central host level. Unique to the access control as a service, model is the use of a communications receiver.

The communications receiver software is designed specifically to accept remote Keyscan panel connections via the internet. In this mode the communications receiver is assigned a static IP address that access control panels deployed at customer sites use to connect to the Central Host.

**CMAC Single client deployment**

Designing the central host typically requires two servers to optimize overall system performance.

A Keyscan database server is dedicated to run and support the Keyscan database with backup provisioning while a second server is dedicated to run the Keyscan communication receiver software. It is the communications receiver software that will listen for remote client panels and permit connectivity once the panel identification is validated with the Keyscan Database.

Once connectivity to the panel is established, the host will maintain the connection indefinitely. This unique Keyscan design ensures that up to the moment transactional data is maintained in the central database for instant report generation, and system edits such as cardholder additions or deletions.

Keyscan's AUR-WEB application rounds out the access control as a service offering allowing central station/integrators the opportunity to provide their clients with a website portal so they may run reports, unlock doors and manage their access control systems without onsite servers.


CMAC eliminates costly computer infrastructure typically required for Access Control but also the dedicated staff needed to manage it, lowering your expenditures.

# Central host administration


Keyscan's central host database ensures complete data autonomy between end-user sites. As new client sites are brought online they are assigned their own site or customer identification to facilitate data integrity and complete isolation between clients.

The integrator/central station maintains a master login account that provides full privileges for all of their managed accounts/sites. Logins for the end-user may be created with limited privileges or site limitations at the discretion of the integrator/central station administering the access control service. With infrastructure in place the integrator/central station now have the ability to create one or a variety of full service maintenance packages to suit their client's needs and expectations.

A variety of monthly maintenance packages may offered along with their associated monthly fees. In some instances the integrator/central station may provide an advanced service for credential issuance that includes printing employee photo badges. Access control as a service offers maintenance free benefits for end-users while offering the very best in access control.

**Software as a service (SAAS)**

**Easy IP Configuration**

**No on-site server/PC required**

**Utilized the same hardware**

**No database maintenance**

**Lower up-front costs**

**System design - Independent client system maintenance**

Keyscan offers an Aurora web application (AUR-WEB) that augments the integrator/central station host design topology. The AUR-WEB application essentially serves up an access control software management webpage.

The AUR-WEB application provides a solution for those end-users that wish to perform basic administration of their access control system. As a result, AUR-WEB is the single most important factor to drive recurring revenue. With the AUR-WEB software users are provided with a site name, login and password to access their site portal via any internet connection.

This login information provides the user with specific access to their system and permits them to add, delete or modify card holders, change access levels, lock/unlock or pulse doors and run the full breadth of system reports when and as they require, to manage their system.

AUR-WEB requires fully licensed and functioning Keyscan Aurora software.

# System design customer sites/Accounts

System administrators typically, are very restrictive regarding the incoming traffic they allow on their network. This is because inbound traffic can be harmful, compromising the LAN and exposing it to malicious activity. Keyscan has adopted a communication process where the panel initiates outbound communications with its designated host. IT system administrators are typically less restrictive when it comes to out-bound connections via the internet resulting in dramatically simplified site installations.

The access control system is installed as normal at the end-user location. The panel is fitted with, a NETCOM6P, AES encrypted Ethernet adapter to provide maximum communications security. The panel is then programmed locally with the central station host IP as well as a backup central station host IP for fault redundancy.

Once the NETCOM6P Ethernet adapter is connected to the end-user LAN (a LAN that offers a port to the internet) the panel proceeds to connect to the defined host IP. In all cases the panel initiates connectivity with the host communications receiver. This allows for DHCP assignment of an IP on the NETCOM6P, ensuring that the NETCOM6P is auto recognized on the end-users established subnet.

This system design establishes the Keyscan panel as a network appliance. An auto-reconnect feature permits the panel to re-establish connectivity with the host if the internet connection drops out for any reason. In the event of connectivity failure, the panel remains fully operational while new card additions and other system changes are queued at the hosts communication receiver to be downloaded once the panel auto re-establishes connection.

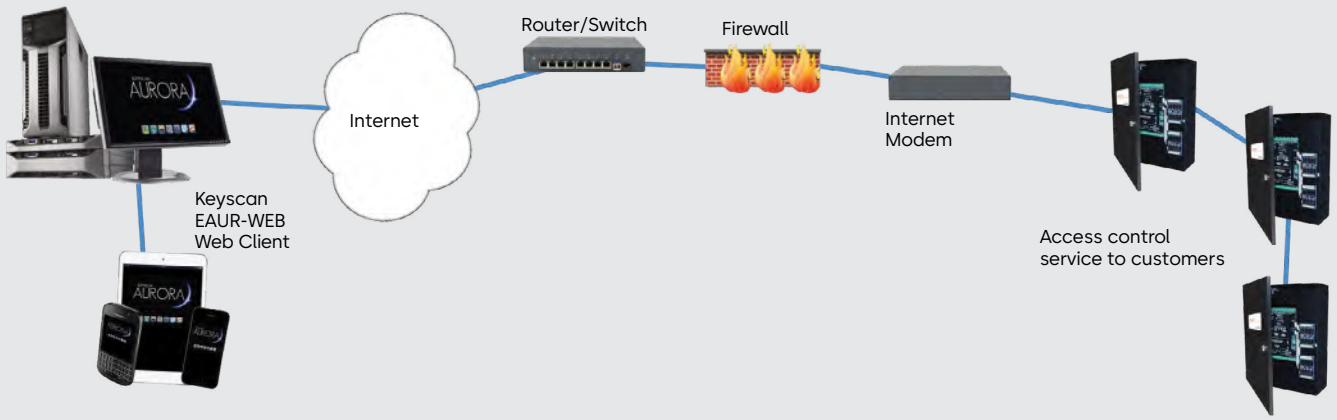
**System expansion**

Keyscan fully supports exponential grow for the integrator/central station and is designed to fully leverage the critical infrastructure required for the initial host implementation. Keyscan created a flexible account expansion software license (EAUR-RN) that seamlessly allows an increased amount of reverse network connections to the host database.

The EAUR-RN License increases the number of host connections by ten additional connections. An unlimited number of EAUR-RN licenses may be added to economically support account expansion. Loading and performance criteria must be reviewed periodically to ensure optimal host infrastructure performance.

**Access control service to customers**

Diagram for informational purposes only. Actual implementations may vary.



# Single or multi-panel sites

Keyscan's full lineup of access control units support centrally managed access control.

- CA150 Single-door controller
- CA250 2 reader controller
- CA4500 4 reader controller
- CA8500 8 reader controller
- EC1500 1 Cab Elevator controller
- EC2500 2 Cab Elevator controller

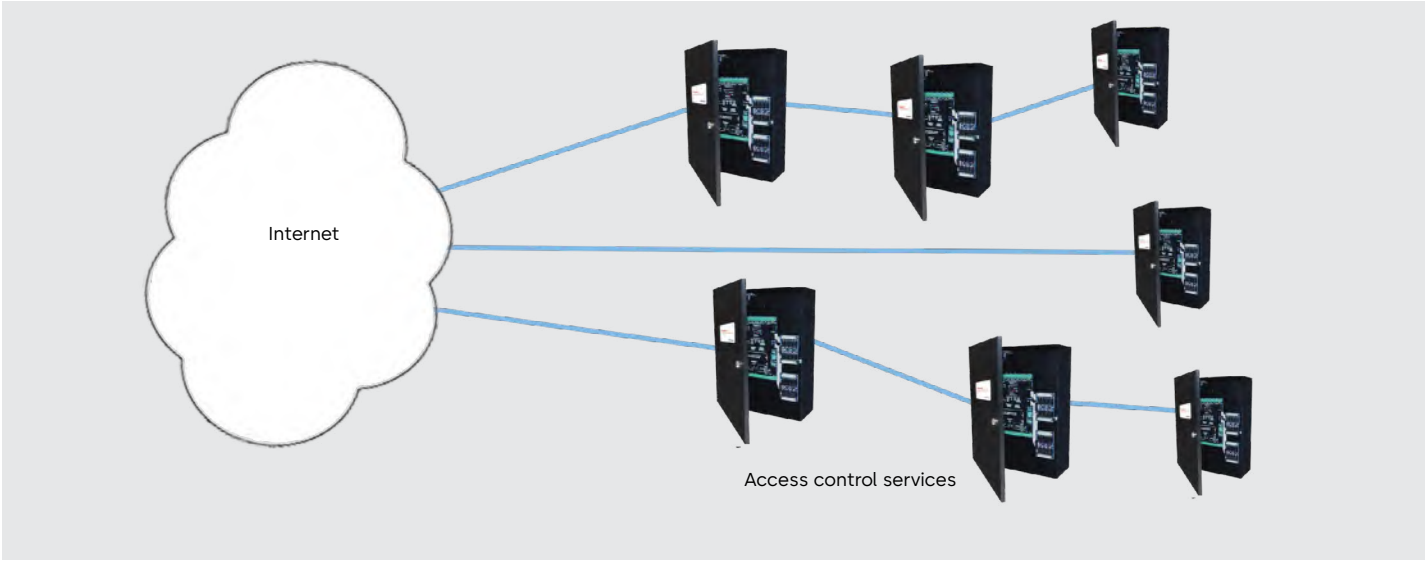
Panels may be mixed and matched at the customer location to optimize the installation for their site based on the total number of doors to be secured with access control.

This total system design flexibility provides the integrator/central station with a comprehensive access control service solution for both small and large end-user installations.

**Multiple branch/Offices**
End-users with multiple locations within the same city, the continental United States or international facilities can benefit from Keyscan centrally managed access control solution and leverage the internet for their access control connectivity.

By selecting a facility and equipping it with the necessary infrastructure to function as the central host, a company, large or small, can establish a centrally managed access control system for their enterprise.

Branch offices may use AUR-WEB to conduct branch specific maintenance and run necessary reports. The corporate office can offer as much or as little capabilities for the branches offices as deemed appropriate.




EAD_1802_BR_EN CEI 0525
Subject to change without notice

**dormakaba USA Inc.**

6161 E. 75th Street
Indianapolis, IN 46250
1-888-539-7226

**dormakaba.us**

**dormakaba.com**