



802.1x Implementation in Printers

- Required to set up an in-house secure network infrastructure
- Complete ownership from concept to implementation

Situation

Network Administrators traditionally managed external and internal threats through access rights and firewalls. In today's co-operative networks, it has become important for administrators to identify and provide appropriate access to devices as well as users. An emerging standard in this respect has been 802.1x.

The 802.1x protocol provides a mechanism for authenticating approved devices through approved physical network ports. Since the 802.1x is customizable, administrators have the ability to provide full/limited access to the network, depending on the user's authenticating.

For a leading document management technology and service enterprise, there arose a need to implement 802.1x, an emerging network security standard on MFP devices, which would allow the client to sell its devices in markets where network security is important.

Challenge

- The challenge was to first set-up an in-house secure network infrastructure using 802.1x, which the development and testing teams could leverage. The secure network had to be interoperable between different authentication schemes and network topologies.
- 802.1x needed a robust certificate management implementation on the device. It had to scale down OpenSSL implementation with a smaller footprint for the embedded device.
- The team of engineers implemented support for four different authentication schemes and made sure that they were interoperable.

Celstream Response

Celstream's team took complete project ownership from concept to implementation. In minimal learning time, the team gained expertise in 802.1x technology and its different authentication protocols. In addition to these, the team also participated with the customer in developing requirements for this feature. Initially, the 802.1x infrastructure was set-up for the development team and subsequently, a comprehensive one was set-up on the main network for the test teams.

In addition to these, the following authentication protocols were also implemented:

- MD5
- PEAP
- EAP-TLS
- Implemented the 802.1x configuration on the embedded web server

Case Study Highlight

Celstream has been able to showcase its engineering capability in developing the security stack, based on emerging standards. This solution opens up the high value “Secure Networks” market segment for the client. This market segment is a new initiative for the client and is an integral part of its business strategy.

Technology

In developing this solution, Celstream used the following key software platforms:

- Windriver 802.1x stack
- OpenSSL for certificate management
- RomPager® embedded web server
- Microsoft Internet Authentication Server
- FreeRADUIS server

Copyright© 2014, Celstream Technologies Private Limited. All Rights Reserved. Printed in India. The information in this publication supersedes that in all previously published material. Specification and price change privileges reserved. For the most up-to-date information, please visit our website at www.celstream.com.

Celstream is a trademark of Celstream Technologies Private Limited. RomPager is a registered trademark of Allegro Software Development Corporation. All other trademarks are the property of their respective owners.

All prices, specifications and characteristics set forth in this publication are subject to change without notice.

For further information, please contact Celstream:

USA
Ph: +1 877 ASK CELSTREAM (275-2357)
Fax: +1 (503) 293 3578
Email: sales.usa@celstream.com

INDIA
Ph: +91 (80) 6740 4040
Fax: +91 (80) 6740 4100
Email: sales.india@celstream.com

AUSTRALIA
Ph: +61 (0) 2 9416 0475
Fax: +61 (0) 2 9416 2583
Email: sales.australia@celstream.com