

Until recently, electronic offline locks were the only part of an access control system that were still proprietary. With the trend to merge security solutions and card technologies, the demand for a standard solution for the process of writing authorisations to a card has grown. That's when four companies started working together to create a new standard; Standard Offline Access Application (SOAA).



'Card technologies have become standard instead of proprietary. We see a shift from having to support multiple card technologies to a few selected card technologies, such as MIFARE, Legic and UHF. For online access control we solve the problems of different card technologies and their programs by having our software running on controller level. But for offline access control we saw that, although the card technologies were the same, each manufacturer has its own proprietary way to write access right on the cards. That's why we think that the next step for this market will be standardisation like ONVIF was for IP Video Cameras. In the near future, customers will ask for a generic and secure way to bring authorisation rights on a card which can be used independent from the wireless offline locks.'

Nedap Security Management
Arjan Bouter, Sales Director



Opening new doors

IP and IT convergence within the security industry is an ongoing process. Hardware products have become native IP devices where software determines their functionality. One of the results is that the market is demanding standardisation. An example of this is the introduction of the ONVIF standard for IP Video cameras. For offline wireless locks, we have reached the point where they can no longer be proprietary.

Breaking the barriers

At the moment it's difficult for customers to manage several brands of offline wireless locks with one system and use a single card technology. That's why the initiative to establish and maintain a standard for authorisation rights on a card for the most common card technologies was taken. This standard should be able to integrate offline wireless locks easily into security management (access control) systems. One of the initiators of this standardisation, Frederik Hamburg, notes, 'Some large companies like Airbus

and Frankfurt Airport came to talk to us at the Legic partner seminar in Switzerland. If you look at these organisations, you're talking about 40,000 offline wireless locks or more. Once they bought the first 10,000 locks from a single supplier, the next 10,000 will cost even more, because you have to stay with them anyway. That's why the demand has grown for a standard encoding solution, in order to free customers from being in the hands of one single supplier. As Zugang GmbH has done these kind of standardisation projects before, we amongst others started the initiative and looked for suppliers to work out the technical specification for the standard.'

Markus adds, 'It was only a matter of time before customers would ask for this standard. You see that customers want future proof and flexible products, and that means they also want to have freedom of choice, now and in the future.'

When asked if this standard is only beneficial for large international companies, Frederik says, 'Large companies will especially benefit from standardisation. Now

they are going global, they see the problem that all their local sites have different lock-solutions, all with different ways of writing data to the card. They need a solution to write the authorisations to the card on the same way at every site in the world. Only then will they be liberated from the fortress of suppliers, and also smaller companies benefit from this.'

Unlocking the benefits

According to Arjan Bouter, 'By having this standardisation, customers will be able to use multiple wireless offline locks from multiple suppliers and handle them in one security system in the same way. This is user friendly for those who have to manage the authorisations and convenient for the card user. It also

makes the integration of offline locks easier.' Anton notes, 'Once the customer has integrated one offline lock system, he has integrated all.' Frederik adds, 'With wireless offline locks, you can save investment on the infrastructure like cabling or wireless access points. For doors which are in areas where not many people enter, or the security can be downsized instead of being monitored real time, or cabling and wireless is impossible, the electronic offline lock is a perfect solution. Thanks to SOAA this becomes a standard and will enable customers to save costs on integration and allow them to choose the right product. In the end, the customer is free to decide which solution fits best, given the circumstances.'

'Wireless locks are an economical solution. Purchasing a mechanical lock might be cheap, but costs for long-term maintenance are often high. Nevertheless, companies who implement wireless locks should be aware of what they are doing. Not every door is suited for a wireless lock, this is also true for mechanical locks. As a consultant, my role is to help the customer define what the scenario for each door is in terms of how many people go through it every day and the required level of security.'

Zugang GmbH
Frederik Hamburg, Consultant



'Online, wired doors only cover 10–20 percent of the the doors in a building nowadays, mostly the high secure doors. Other doors, mostly those within the buildings, are traditionally fitted with mechanical locks. There is a tendency to control these doors as well, so that less mechanical keys – which have additional maintenance costs are necessary anymore. Therefore wireless locks are on the increase. We can meet customer demand to merge offline wireless locks within our security management system, so that they can be controlled from one single platform.'

Nedap Security Management
Anton Kuip,
Technical product developer AEOS

Reliable, proven technology

Frederik proceeds, 'By introducing this standard, the customer gets freedom of choice. But more importantly, it's also more secure. We see a shift from facility departments to IT departments buying the solutions, therefore requiring open standards and proven technologies. Customers want a transparent solution, they want to be able to see what it does.' Anton adds, 'Proven technologies are the most secure. Standards are open and therefore tested and investigated by everyone, including hackers. This is the most secure way.' Markus confirms, 'When technology is standard, the only thing that they have to worry about is the looks and price. They can pick the best and most secure solution out of a wide range of products, even mixing and matching them from different suppliers.'

Freedom of choice

'Our vision is that customers should get the best security solution for their situation and that hardware must never limit the options,' Arjan continues. 'Nedap has developed its security management platform AEOS as an open standard security solution. We stay up to date with technologies that could integrate in our platform and we have already integrated third party offline wireless locks.' Assa Abloy also wants to open the market for freedom of choice in wireless locking solutions, for instance Aperio from Assa Abloy. Frederik will be happy when more suppliers support this, as second source buying is a real customer benefit; not only because of the freedom of choice, but also because standardisation will result in reduced prices.

Standardising the standard

In order to get that freedom of choice, customers have to specify this. Arjan Bouter states, 'Customers appreciate this initiative and see the added value of it. They're actually waiting for it, claiming that they will no longer invest in proprietary solutions with this new standard coming up.' Frederik Hamburg adds, 'Tendering is an important step in the process of getting the standardisation accepted. This means that customers, after having seen the specifications, will ask for the SOAA standardisation in their tenders.' Markus confirms this, 'A customer should ask for SOAA compatibility in their tenders. If they don't, then that's a risk for the success of the standard.'

When asked about the current status of the project, Frederik says: 'We have finished the technical specifications. Zugang GmbH shared these specifications with other offline wireless locks supplying companies. Having seen these specifications, approximately 10 of them confirmed that they will implement SOAA once the market asks for it. In order for a standardisation to become successful, enough suppliers need to follow, otherwise there is no competition. The customer benefit is that prices will decrease and they gain greater freedom of choice.'

'Our customers don't want to have to change RFID cards when implementing offline wireless locks. That's a hassle. That's why our wireless locks should standardly support every RFID technology. On the other hand, the demand towards architectural ranges, i.e. colours, handles, etc in different variations is increasing. In other words, customers ask for standardised technology with customized design.'

ASSA ABLOY
Markus Henkelmann,
Portfolio manager electronic access control

