OVERVIEW

In this document we will lay out the different types of credentials in the access control market. Access credentials are a subset of RFID credentials. RFID tag and signals range far beyond access control. Frequencies and readers will be explained in other documents.

The format lengths described how the card number is used. If you saw a number like 549030933 or 5128475024 you wouldn't have any context to how that number operates in the real world. If you knew the first one was a social security number and the second one was a phone number, then it would make perfect sense. For the phone number, the first 3 numbers "512" are your area code. Let's keep this example in mind as we explore the format lengths.

26-BIT FORMAT

This is an open format meaning that each 26-bit card is read the same, card number (5 digits) and facility code (3 digits). The bit length refers to the number of bits if the number was broken down into binary code.

There are 16.7 million unique cards for the 26 bit format. There are two numbers on the card that make it unique, facility code (0 - 255) and card number (1 - 65,535). They are unencrypted numbers that are passively transmitted between the card and the reader (more about this in frequencies). The "area code" of the card is in the same place every time, just like it is with your phone number. This is why the 26 bit format is "standard".

Common applications of these credentials are doors with low security needs and most legacy systems. It is a very common card type and still widely used today. These cards work within the low frequency range of 125kHz. This is a passive communication, meaning the card does not need a battery or power to transmit the signal. The reader is constantly looking for/ accepting credentials within that frequency range.

OTHER BIT FORMATS

We moved away from the "standard" format and now we have 100s of different "formats" for varying bit lengths. The "area code" is not going to be in the same location every time. Each manufacturer might place the "area code" differently. Once might place it in the middle of the number string, while another might place it at the end. Each manufacturer will have their own format that they follow.

More than just the placement of the "area code", these different formats also utilize something called a "parity" bit. Parity bits tell the device (door controllers) if the data being received is accurate. The manufacturer will decide if the bit should be even or odd to be deemed as accurate. These parity bits allow for higher security credentials. It makes the card harder to duplicate. Not only do you need to know the "area codes" placement, you will also need to know the parity bit placement and if it should be a 1 or a 0.

As the card bit length increases two things will increase as well. Total number of unique credentials as well as number of parity bits in the number string. The more the parity bits there are, the hard it is to duplicate the credential.

For more information or questions about bit lengths - please reach out the the BlueWave Support team at Support@bluewavesecurity.com

Related Documents: Mobile credentials, Card/ Reader Frequencies,Wiegand vs ODSP