



ENTRUST

A

B

Challenge

Antel, Uruguay's state-owned telecommunications company, manages the country's entire landline telephony and is its leading mobile and data operator. The company was facing a significant challenge in identifying and authenticating its users in the digital context, particularly for electronic signatures and transactions. This was a complex task due to the need for high security and reliability in a digital environment.

Solution

Entrust provided a comprehensive solution to Antel's challenge. The solution involved the implementation of Entrust Remote Signing Server (RSS) and Entrust nShield Hardware Security Modules (HSMs). These technologies enabled Antel to securely manage digital identities and perform electronic signatures. The solution also included the implementation of Entrust PKI solutions to ensure the integrity and confidentiality of digital communications.

Results

The implementation of the Entrust solution resulted in several key benefits for Antel. First, it enabled the company to confidently identify and authenticate its users in the digital context, significantly reducing the risk of fraud and identity theft. Second, it facilitated the mass adoption of digital identification and electronic signatures, which is essential for the growth of digital services. Finally, the solution established trust in electronic signatures, which is a critical factor for the success of digital transactions.

CUSTOMER PROFILE

Antel, Uruguay's state-owned telecommunications company, manages the country's entire landline telephony and is its leading mobile and data operator.

Objectives

- Confidently identify human users in the digital context
- Implement identification and authentication processes across combined technologies
- Encourage mass adoption of digital identification system and establish trust in electronic signatures

Technology

- Entrust Remote Signing Server
- Entrust PKI solutions
- Entrust nShield HSMs



A

A

Creating a safe, easy-to-use system for identification and authentication

As a result of the COVID-19 pandemic, many organizations have had to rapidly implement remote access solutions for their employees. This has led to a significant increase in the use of virtual private networks (VPNs) and other remote access technologies. While these solutions have been essential for maintaining business continuity, they have also introduced new security risks. One of the most significant risks is the potential for credential theft and unauthorized access. This is where a secure and easy-to-use system for identification and authentication becomes crucial.

A secure and easy-to-use system for identification and authentication is essential for protecting sensitive data and ensuring that only authorized users can access organizational resources. This system should be designed to be user-friendly, secure, and scalable. It should also be able to integrate with existing systems and provide a seamless user experience. The system should be able to handle a large number of users and provide a high level of security. This is where a secure and easy-to-use system for identification and authentication becomes crucial.

The system should be able to handle a large number of users and provide a high level of security. This is where a secure and easy-to-use system for identification and authentication becomes crucial. The system should be able to handle a large number of users and provide a high level of security. This is where a secure and easy-to-use system for identification and authentication becomes crucial.

Navigating technical challenges

C. The first step is to identify the problem. This involves understanding the current state of the system and the desired state. Once the problem is identified, the next step is to develop a plan to address it.

- D. The second step is to analyze the problem. This involves breaking down the problem into smaller, more manageable components. This allows you to focus on one aspect of the problem at a time and develop a solution for each component.

- G. The third step is to implement the plan. This involves putting the solution into action. It is important to monitor the progress of the implementation and make adjustments as needed. Once the plan is implemented, the next step is to evaluate the results.

- E. The fourth step is to evaluate the results. This involves comparing the current state of the system to the desired state. If the results are not as expected, you may need to go back to the analysis phase and re-evaluate the plan.

- F. The fifth step is to document the process. This involves recording the steps you took to solve the problem. This documentation can be useful for future reference and for sharing your knowledge with others.

(BD 2 0), () () 1 () 2、 () 1 () () 2、

- I...
H. M.,
- P... API
E... PKI
I...
E... PKI
A... N...