WHITE PAPER

How Xiid Secures Electric Vehicle Charging Infrastructure

Executive Summary

The rapid expansion of electric vehicle (EV) charging infrastructure has introduced unprecedented cybersecurity challenges that threaten not only individual charging stations but the stability of entire power grids. Recent data reveals a dramatic 39% increase in cyberattacks against automotive and smart mobility ecosystems in 2024. 60% of these attacks had the potential to affect millions of devices, highlighting the massive scale of vulnerability across interconnected charging networks. The consequences extend far beyond individual inconvenience—compromised charging stations can serve as entry points for grid manipulation, data theft, and even physical infrastructure damage.

Xiid's Terniion™ addresses these evolving threats through its groundbreaking SealedTunnel™ technology, which fundamentally reimagines how critical infrastructure is secured and exceeds Zero Trust principles. By eliminating traditional attack vectors through closed firewalls, implementing quantum-secure cryptography, and providing credential-less authentication, Xiid delivers comprehensive protection that exceeds current industry standards while futureproofing against emerging threats.

The Growing Cybersecurity Crisis in EV Charging

Electric vehicle charging infrastructure represents a convergence of multiple complex systems: power generation and distribution, financial transactions, user data management, and grid coordination. This complexity creates numerous attack surfaces that malicious actors are increasingly exploiting with sophisticated techniques.

The Scale of Current Threats

Security researchers have documented an alarming escalation in both the frequency and sophistication of attacks against EV charging infrastructure. Tens of thousands of charging stations across Europe and North America are likely to contain critical security vulnerabilities, and attacks specifically targeting EV charging infrastructure are quickly growing.

These statistics reflect not merely an increase in opportunistic attacks but a fundamental shift in how threat actors view EV charging infrastructure. What was once considered a niche target has become a primary vector for accessing broader energy networks, financial systems, and personal data repositories.

The Expanding Attack Surface

Modern EV charging stations are far more complex than simple power delivery systems. They integrate payment processing capabilities, user authentication systems, grid management protocols, and remote monitoring capabilities. Each of these components introduces potential vulnerabilities that attackers can exploit.

Payment systems within charging stations store financial data and process transactions, making them attractive targets for fraud and identity theft. Communication protocols between charging stations and backend management systems often lack adequate encryption, allowing attackers to intercept sensitive data or inject malicious commands. Grid integration features that enable demand response and load balancing can be manipulated to create artificial demand spikes or destabilize power distribution networks.[3]

Perhaps most concerning is the interconnected nature of modern charging networks. A successful attack on one charging station can serve as a launching point for broader network compromises, potentially affecting thousands of devices across multiple geographical regions. This interconnectedness means that the security of any individual charging station directly impacts the security of the entire network.

Xiid's Approach to True Zero Trust Protection

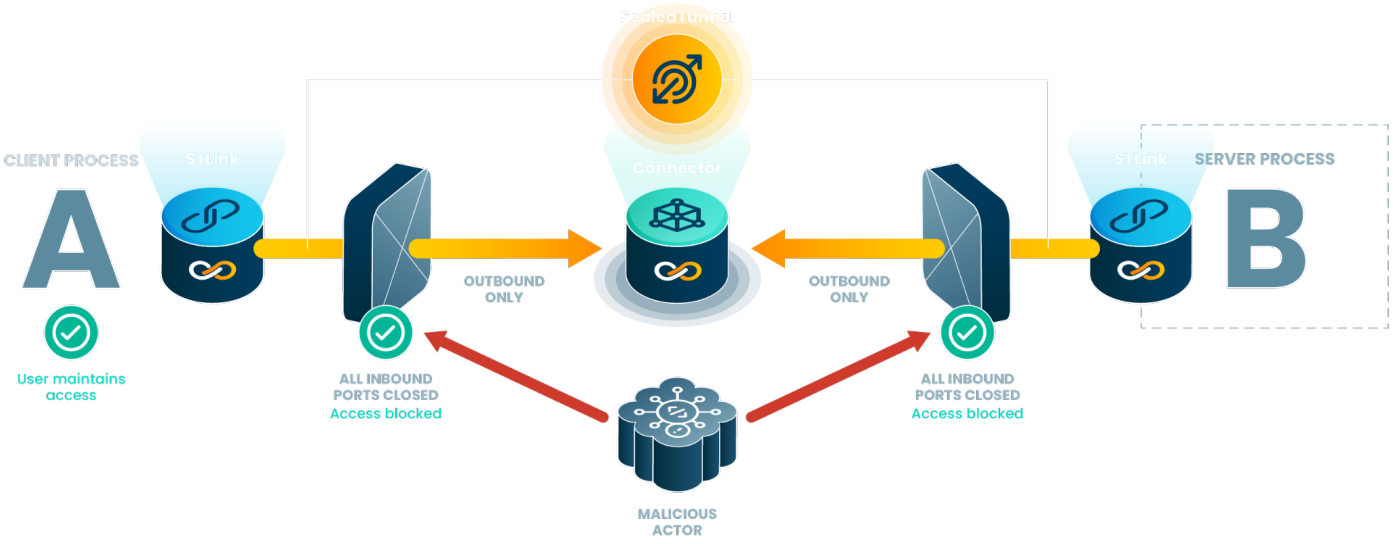
Traditional cybersecurity approaches rely on creating barriers around networks and trusting internal communications once authentication is established. However, this perimeter-based security model has proven inadequate for protecting modern, interconnected infrastructure like EV charging networks. Terniion fundamentally reimagines security by eliminating trust assumptions and removing attack surfaces rather than simply defending against them.

Core Principles of Secure by Design

Terniion represents a paradigm shift from defensive to preventive security. Rather than accepting that networks will have vulnerabilities and attempting to monitor and respond to threats, we exceed Zero Trust principles to eliminate the pathways through which attacks can occur. This approach is built on several foundational principles that distinguish it from traditional Zero Trust implementations.

Xiid Terniion eliminates attack surface by allowing all inbound ports to be closed, making network, IoT, and other resource infrastructure non-addressable. This makes it extremely challenging – if not impossible – for an attacker to leverage any attacks in their arsenal as they would be unable to see or reach their target device. Additionally, Xiid never stores sensitive customer data or identities, and multiple layers of end-to-end, quantum-secure encryption using NIST "gold standard" algorithms ensure that neither Xiid nor any other third party can ever view data in transit.

Xiid credential-less authentication tool, Aclave™, leverages Zero Knowledge Proofs and one-time-codes to authenticate users without ever transmitting sensitive identity information over the internet. This ensures that IoT devices can only be accessed by authorized parties, and by eliminating credentials, eliminates the risk of phishing attacks. Xiid's robust solution for credential-less authentication has been awarded several U.S. patents (US20220263817A1, US11991287B2, US20200267139A1).



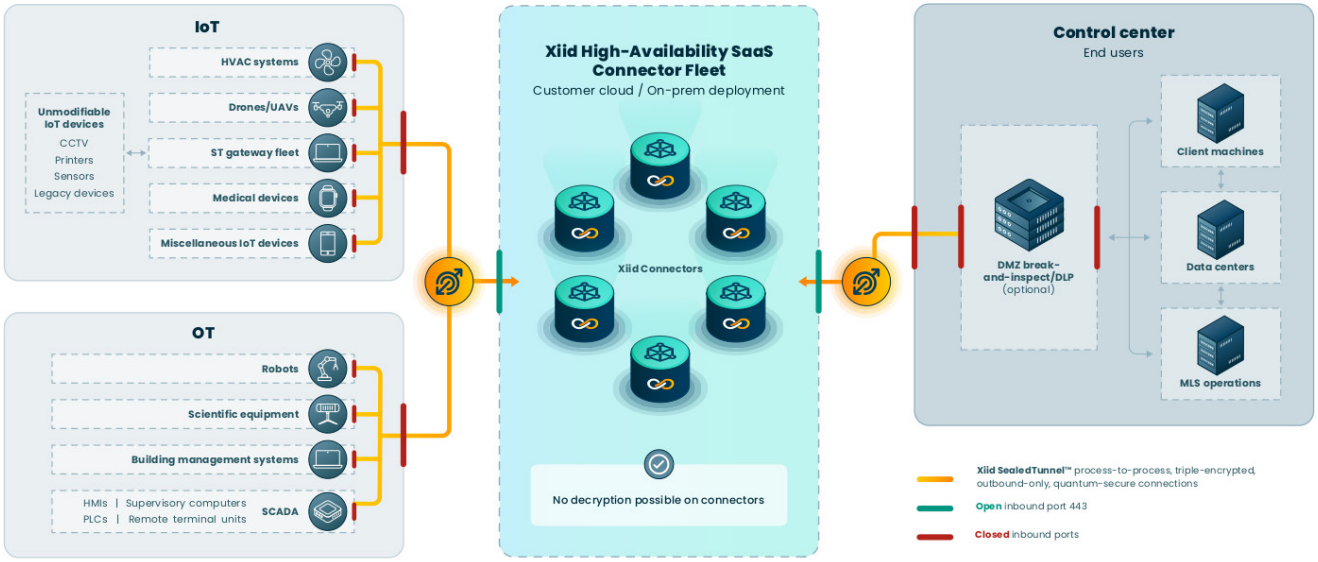
XIID OUTBOUND-ONLY AUTHENTICATION AND ACCESS WITH CLOSED FIREWALLS

SealedTunnel Technology for Secure Communications

Xiid's SealedTunnel technology establishes process-to-process communication channels that operate exclusively through outbound connections. Traditional VPN and tunnel technologies often require endpoints to accept inbound connections, creating potential attack vectors. Terniion eliminates this vulnerability by ensuring that all communication flows originate from protected resources and travel outbound.

Critically, Terniion utilizes quantum-secure algorithms (Kyber key encapsulation and Dilithium digital signature), future-proofing data from future threats such as “Harvest Now, Decrypt Later”. In addition, it’s built to work robustly on “dirty”, hostile, and degraded networks with industry-leading packet delivery.

All Xiid solutions are fully interoperable with zero configuration across different types of networking infrastructure (ORAN, satellite, cellular, etc.) and are also location-independent, meaning that physical devices and infrastructure can be moved thousands of miles or across continents and continue to function as expected without intervention.



IOT/OT MICROSEGMENTATION WITH XIID TERNIION

Traditional network security approaches attempt to create secure perimeters around groups of resources, but this approach has proven inadequate for protecting complex, interconnected infrastructure like EV charging networks. Once attackers breach the perimeter, they can often move freely within the protected environment, escalating privileges and accessing additional resources.

Xiid’s approach implements microsegmentation at the process level, creating isolation boundaries around individual application processes rather than larger network segments. This granular segmentation ensures that even if one component of a charging station is compromised, attackers cannot use it to access other processes or systems.

The microsegmentation architecture is particularly important for EV charging infrastructure because charging stations often integrate multiple independent systems: payment processing, user interface management, power delivery control, communication handling, and monitoring functions. Traditional security approaches might protect these systems as a single unit, meaning that compromise of any component could lead to compromise of all components.

Process-level microsegmentation ensures that payment processing systems cannot access power delivery controls, communication systems cannot access user interface components, and monitoring functions operate in isolation from operational controls. This approach significantly limits the potential impact of any individual security breach and prevents attackers from escalating access across system boundaries.

Protecting Charging Station Communications and Payment Systems

EV charging stations must communicate with multiple external systems to function properly: backend management platforms for monitoring and control, payment processing systems for transaction handling, grid management systems for load coordination, and mobile applications for user interaction. Each of these communication channels traditionally requires network connectivity that creates potential attack vectors.

Terniion eliminates these vulnerabilities by ensuring that all charging station communications occur through outbound-only SealedTunnels.

This architecture provides several critical security benefits. First, charging stations become completely invisible to external reconnaissance efforts since they maintain no open inbound ports or public IP addresses. Second, all communications are protected by multiple encryption layers, including quantum-secure algorithms that protect against future threats. Third, the process-to-process architecture provides segmentation between charging stations and their networks, preventing direct attacks against and lateral movement through charging infrastructure.

The outbound-only communication model also enables charging stations to operate securely even when deployed in hostile network environments. Whether connected through cellular networks, public Wi-Fi, or other potentially compromised communication channels, the encryption and authentication mechanisms ensure that communications remain secure and charging stations remain protected.

Grid Integration and Energy Management Protection

Modern EV charging infrastructure plays an increasingly important role in electrical grid management through demand response programs, load balancing, and integration with renewable energy sources. These grid integration features require charging stations to communicate with utility systems and respond to grid management commands, creating additional attack surfaces that malicious actors can exploit.

Attackers who successfully compromise grid integration communications can manipulate charging loads to create artificial demand spikes, coordinate attacks across multiple charging stations to destabilize power distribution networks, or interfere

Tested and Proven Unreachable

Xiid's Terniion solution with Aclave credential-less authentication is proven to deliver military-grade cybersecurity and network protection and both are already in use within the U.S. Department of Defense, achieving a full Authority to Operate (ATO) through the Defense Health Agency (eMASS N-3551). This was further validated by a penetration test performed on Xiid's products by the U.S. Air Force Research Laboratory (AFRL), and not only was the AFRL unable to breach Xiid's encryption, but their tests also demonstrated the "...near invisibility of the product externally."

with demand response programs that help maintain grid stability. The potential for such attacks to cause widespread power outages or grid instability makes securing these communications critical for national infrastructure protection.

Terniion provides comprehensive protection for grid integration communications through the same outbound-only, triple-encrypted channels used for other charging station functions. Grid management commands and data exchanges are protected by quantum-secure encryption and transmitted through platform architecture that prevents interception or manipulation by external attackers.

The architecture also provides natural isolation between charging stations and utility networks, preventing compromised charging equipment from serving as entry points for attacks against broader electrical infrastructure. Even if individual charging stations are compromised through physical access or other attack vectors, Terniion can prevent attackers from using these compromised systems to access utility networks or launch attacks against other charging stations.

Resilience Against Infrastructure Attacks

EV charging infrastructure operates in challenging environments where network connectivity may be unreliable, hostile, or subject to interference. Charging stations must continue operating securely even when deployed in locations with poor network infrastructure, limited physical security, or active cyber threats.

Xiid's solution is specifically designed to maintain security and functionality even in degraded network environments. Our patented technology includes advanced packet delivery mechanisms that ensure reliable communication even over "dirty" networks. The system can adapt to varying network conditions, automatically adjusting communication parameters to maintain connectivity while preserving security.

The outbound-only communication model provides natural resilience against network-based attacks. Since charging stations never accept inbound connections, network-based denial-of-service attacks, port scanning, and other reconnaissance activities cannot directly target charging infrastructure. Even if surrounding network infrastructure is compromised, charging stations remain protected through their encrypted outbound communication channels.

Industry Standards Compliance and Best Practices

The cybersecurity of critical infrastructure is governed by numerous industry standards, government regulations, and best practice frameworks. Xiid's approach to EV charging security is specifically designed to meet and exceed these requirements while providing additional protections that address emerging threats and evolving attack techniques.

Xiid's cybersecurity solutions are meticulously aligned with and frequently exceed the latest industry best practices, including the NIST Cybersecurity Framework (CSF) 2.0 and the CISA Cybersecurity Performance Goals (CPGs). Xiid's platform is architected to exceed these rigorous federal guidelines, providing comprehensive protection tailored to critical infrastructure environments.

These frameworks are operationalized by mapping Xiid's security controls, processes, and risk management strategies to NIST CSF 2.0's core functions: Govern, Identify, Protect, Detect, Respond, and Recover. In addition, Xiid actively supports the implementation of CISA's CPGs by prioritizing and enabling controls such as multi-factor authentication, including FIPS 140-2 and NIST Authenticator Assurance Level

(AAL) 1-3 compliance, network segmentation, secure backups, vulnerability management, and timely patching — ensuring both IT and Operational Technology (OT) environments reach elevated security maturity.

While the CPGs require multifactor authentication, Xiid's Aclave provides credential-less, Zero Knowledge Proof-based authentication that eliminates the risk of credential theft, reuse, or phishing attacks. Microsegmentation, another requirement, is also improved upon by Xiid's process-to-process communications segmenting networks at the process level, rather than the wider device level.

On encryption, the CPGs require "Strong and Agile Encryption", to which Xiid delivers three layers of encryption wrapping all connections, including multiple end-to-end encrypted layers and quantum-secure layers using NIST's post-quantum standards, Kyber key encapsulation and Dilithium digital signature.

On infrastructure that may be vulnerable to attacks such as Distributed Denial of Service (DDoS), and its Slow Loris variant, Xiid's platform is engineered to take an active approach in mitigation, preserving resiliency and reliability.

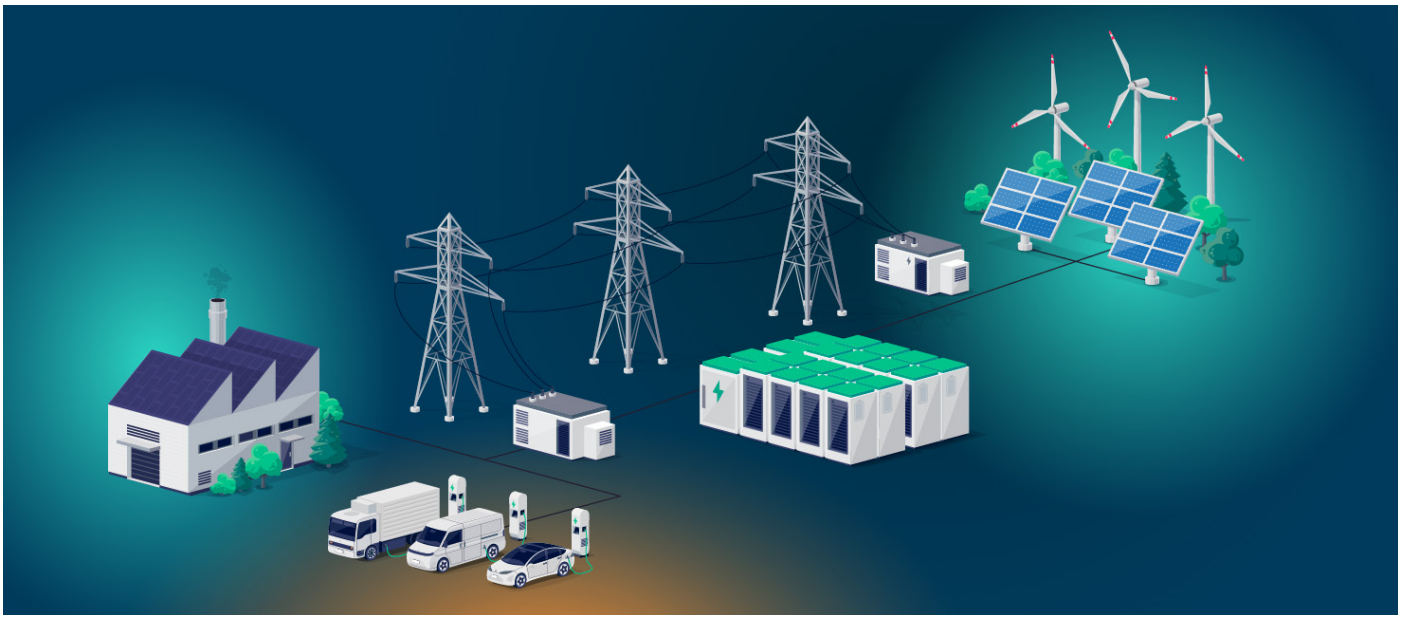
By reliably aligning with, executing on, and exceeding industry best practices, Xiid not only safeguards critical government systems but also provides federal stakeholders with confidence in their cybersecurity resilience. Xiid's strategic prioritization of NIST and CISA guidelines empowers agencies to meet evolving threats, fulfill regulatory requirements, and serve as exemplary stewards of the public trust in the protection of national infrastructure.

Compatibility with Existing Infrastructure

Modern EV charging networks often include equipment from multiple manufacturers, communication systems using various protocols, and integration with diverse backend management platforms. Any security solution must work effectively within this heterogeneous environment without requiring wholesale replacement of existing infrastructure investments.

Xiid's software-based approach enables integration with virtually any type of charging equipment regardless of manufacturer, age, or technical specifications. Terniion's components generally operate at OSI Layer 7, providing security for data in transit without requiring modifications to charging station hardware or core operational software.

Legacy charging equipment that lacks the ability to receive software modifications can be protected through gateway-based implementations where Xiid components are deployed on separate devices that handle all external communications. This approach enables organizations to secure existing infrastructure investments while planning for eventual equipment upgrades.



Scalability and Performance Considerations

EV charging networks are experiencing rapid growth as electric vehicle adoption accelerates. Security solutions must be capable of scaling to support thousands or tens of thousands of charging stations while maintaining consistent performance and security effectiveness.

Xiid's cloud-based architecture is designed for massive scalability, with the ability to support unlimited numbers of charging stations without degrading performance or security. Xiid's Connector-based mesh networking model distributes load across multiple data centers and can automatically scale resources based on demand patterns.

Geographic distribution capabilities enable charging networks to expand across multiple regions while maintaining consistent security and performance characteristics. Charging stations automatically connect to the nearest available Connectors, minimizing latency while ensuring redundant connectivity options for reliability.

Migration Strategies and Deployment Models

Organizations operating existing EV charging networks need practical migration strategies that enable gradual implementation of enhanced security measures without disrupting ongoing operations or requiring simultaneous updates across entire networks.

Xiid supports phased deployment approaches that allow organizations to implement Terniion gradually. Initial deployments can focus on the most critical charging stations or those in high-risk locations, providing immediate security benefits while gaining operational experience with the new technology.

The architecture also supports hybrid deployments where some charging stations use Terniion while others continue to operate with existing security measures. This flexibility enables organizations to prioritize security upgrades based on risk assessments and operational requirements while maintaining consistent network operations.

Training and support programs ensure that operational personnel understand the new security capabilities and can effectively manage the enhanced security features. Comprehensive documentation, online training resources, and technical support services help organizations realize the full benefits of Terniion while minimizing implementation challenges.

Hardening the Backbone of EV Mobility

The cybersecurity of electric vehicle charging infrastructure represents one of the most critical challenges facing the energy and transportation sectors today. As EV adoption accelerates and charging networks expand, the potential impact of successful cyber attacks grows exponentially. Traditional security approaches that rely on perimeter defense and reactive monitoring have proven inadequate for protecting complex, interconnected infrastructure that must operate reliably in diverse and often hostile environments.

Xiid's Terniion provides a fundamental solution to these challenges by eliminating attack vectors rather than simply defending against them. Through the combination of closed firewalls, quantum-secure encryption, credential-less authentication, and process-level microsegmentation, Xiid creates a security paradigm that is both more effective than traditional approaches and more resilient against future threats.

The comprehensive nature of this approach addresses not only current cybersecurity challenges but also anticipates and protects against emerging threats including quantum computing attacks and increasingly sophisticated adversaries. By implementing security-by-design principles throughout the development lifecycle and maintaining rigorous operational security practices, Xiid ensures that EV charging infrastructure can continue to operate securely even as the threat landscape continues to evolve.

The proven effectiveness of this approach, demonstrated through independent testing and real-world deployments in demanding environments, provides confidence that SealedTunnel technology can protect critical infrastructure at scale. As electric vehicles become an increasingly important component of global transportation and energy systems, the security of charging infrastructure becomes a matter of national and economic security.

Organizations responsible for EV charging infrastructure have an opportunity to implement truly transformative security capabilities that not only protect against current threats but establish a foundation for secure operations in an uncertain future. Xiid's Terniion provides the technological foundation for this transformation, enabling the continued growth of electric vehicle adoption while ensuring the security and reliability of the infrastructure that supports it.

The transition to sustainable transportation depends on public confidence in the security and reliability of EV charging infrastructure. By implementing comprehensive cybersecurity measures that exceed current industry standards and protect against future threats, organizations can ensure that this critical infrastructure continues to support the global transition to sustainable mobility while maintaining the highest levels of security and operational excellence.

For more information about securing your EV charging infrastructure with Xiid Terniion, visit xiid.com.