digicert® + NEPKI National Energy Public Key Infrastructure

Securing Australia's Clean Energy Future

Why Digital Identity Is the Missing Piece for a Safe, Reliable, Smart Grid

March 2026

The Challenge in Front of Us

Australia's energy system is undergoing one of the most ambitious transformations of any nation on earth. Millions of rooftop solar panels, home batteries, and smart inverters are turning houses into miniature power stations, feeding electricity back into the grid and reshaping how energy is generated, distributed, and managed.

This explosion of new devices creates a challenge, though:

How do you ensure the energy devices connecting to the grid are trusted and operating securely?

4.2M +	300+	16
Homes with rooftop solar	Device manufacturers	Distribution network operators

The public impact on device security:

- When a smart inverter receives a command to adjust its output during a heatwave, the grid needs certainty that the command came from a legitimate source, not a cyber attacker.
- When a battery storage system reports its charge level, the network operator needs confidence that the data is genuine.
- When an emergency backstop order is issued to protect grid stability, every device in the chain must be verified.

Right now, there is no nationally coordinated system for these operations. This is the problem NEPKI (National Energy Public Key Infrastructure) was created to solve, and the reason Public Key Infrastructure (PKI) matters for every Australian.

What Is PKI?

Think of it like a passport system for devices

When you travel internationally, your passport proves who you are. It was issued by a trusted authority (your government), it contains verified information about you, and border officials can confirm it is genuine. If someone presents a forged passport, the system catches it.

PKI does the same thing for devices and digital communications. Every smart inverter, battery, or grid controller receives a unique digital certificate, issued by a trusted authority, that proves the device is what it claims to be.

PKI provides four essential protections that no other technology delivers together:

Authentication

Confirms that a device or system is genuinely what it claims to be, not an imposter or counterfeit.

Encryption

Scrambles communications so they cannot be intercepted or read by unauthorised parties.

Integrity

Protects data and commands from alteration or tampering while in transit.

Non-Repudiation

Creates an audit trail so every action can be traced to its verified source.

This is not theoretical. PKI is the same trusted technology that secures online banking, government services, and every website you visit that shows a padlock icon. It has been protecting critical digital systems for decades. The question is not whether PKI works. It is whether Australia's energy grid can afford to operate without it.

The World Is Already Moving

Australia is not facing this challenge in isolation. Governments and regulators worldwide have recognised that connected devices in critical infrastructure require strong digital identity, and they are mandating PKI as the foundation.

Regulation / Standard	Jurisdiction	What It Requires
EU Cyber Resilience Act (CRA)	European Union	All products with digital elements sold in the EU must implement secure authentication and cryptographic identity. PKI-based certificates are the primary compliance pathway. Enforcement begins 2027.
NIS2 Directive	European Union	Energy operators classified as "essential entities" must implement strong identity and access management. Digital certificate infrastructure is explicitly referenced as a core requirement.
Digital Operational Resilience Act (DORA)	European Union	Financial entities including banks, insurers, and investment firms must implement comprehensive ICT risk management, including secure authentication and cryptographic controls for critical infrastructure. Effective January 2025.
ISO 15118-2 / ISO 15118-20	International (EV Charging)	The Plug and Charge standard for electric vehicles requires PKI certificates for vehicle-to-charger authentication. Vehicles and chargers exchange digital certificates automatically, with no passwords or cards needed.
SAE EVPKI Certificate Trust List	International (EV Industry)	Launched November 2025, this global trust list governs which Certificate Authorities can issue identity credentials for EV charging infrastructure. DigiCert is a founding participant and provides the signing infrastructure.
FDA Device Regulations	United States	Connected medical devices must implement cryptographic authentication and secure communications. PKI certificates are the accepted standard for device identity in healthcare.
CSA Matter Standard	International (IoT)	The Matter smart home standard requires PKI-based device attestation. Every certified Matter device carries a digital certificate proving its authenticity and authorisation and interoperability for the smart home ecosystem.

The pattern is clear: every major regulatory framework for connected devices in critical sectors, from energy to healthcare and finance to transport, is converging on PKI as the foundational layer for digital trust. Australia's energy grid should not be the exception.

What Happens Without Strong Identity: Lessons from Poland

December 2025, Poland: Cyber attackers compromised more than 30 renewable energy installations, including wind farms and solar arrays, deploying destructive wiper malware across operational technology systems.

The attackers, attributed to Russian state-affiliated groups, exploited a fundamental weakness. Many of the targeted installations relied on default login credentials and lacked multi-factor authentication or device-level identity verification. Once inside, the attackers deployed malware that destroyed monitoring and control capabilities across the sites.

While no power outages resulted, operators lost visibility and control of their renewable energy assets for extended periods.

The attack demonstrated what security researchers have long warned:
without strong, cryptographic identity at the device level, renewable energy infrastructure is vulnerable to disruption at scale.

What We Think PKI Would Have Likely Changed

Device authentication

would have likely prevented access using default or stolen passwords. Each device and operator would have needed a verified digital certificate to communicate with the system.

Mutual authentication

would have likely required both sides of every connection to prove their identity, blocking impersonation by attackers.

Encrypted communications

would have likely prevented attackers from intercepting and analysing network traffic to plan their attack.

Integrity verification

would have likely detected the deployment of unauthorised software and malware before it could execute.

Poland's experience is directly relevant to Australia. With 4.2 million solar installations and a rapidly growing network of smart inverters and batteries, Australia's distributed energy resources present a similar attack surface. A coordinated attack on Australian Consumer Energy Resources (CERs) when they're materially contributing to the generation mix will have consequences far beyond lost monitoring data.

Why Australia's Energy Grid Needs This Now

Australia's energy transition creates a unique set of challenges that make centralised digital identity essential.

Scale and Complexity

Distributed/Consumer Energy Resources (such as solar panels, batteries, electric vehicles) have become a significant and complex part of Australia's energy system. The Australian Energy Market Operator (AEMO) forecasts solar capacity will grow from 28.3 GW today to more than 53 GW by 2030. The Clean Energy Council reports more than 4.2 million homes now have rooftop solar, with over 300 manufacturers supplying equipment. Many of these devices also participate in Virtual Power Plants (VPPs), which allow third parties to aggregate and coordinate the operation of large numbers of systems simultaneously.

The Emergency Backstop

As Distributed/Consumer Energy Resources reach meaningful quantities, distribution network operators must establish emergency controls to ensure the energy system remains stable. Australian State Governments and distribution network operators have begun mandating emergency controls through the technical standard IEEE 2030.5 Common Smart Inverter Profile Australia (CSIP-AUS). Practically, this will enable 13 of Australia's 16 distribution network operators to have the ability to issue emergency commands to manage solar generation or discharge batteries to prevent grid overload. This standard requires PKI by default to prevent an attacker from forging backstop commands that could destabilise the grid during a crisis or prevent legitimate emergency actions from reaching devices.

Fragmented Trust

Without a national PKI framework, each of the 13 distribution network operators, each manufacturer, and each platform provider would need to establish its own identity and trust mechanisms. This creates inconsistency, gaps, and enormous duplication of effort. NEPKI provides a single, coordinated national framework that all participants can trust.

What NEPKI Is Building

NEPKI, the National Energy Public Key Infrastructure, is a not-for-profit initiative established to create a nationally coordinated digital identity framework for Australia's energy devices.

In July 2024 Australia's Energy Ministers released a Consumer Energy Resources Roadmap which included a national reform priority to establish a national non-for-profit entity to coordinate PKI to authenticate communications with CER for backstops and then expanding it to manage PKI for other energy services such as EV charging and virtual power plants. As part of delivering this national reform priority, in July 2025, the Australian Competition and Consumer Commission (ACCC) granted conditional authorisation for NEPKI's operations, enabling the procurement of a PKI service provider to deliver a national PKI service for CSIP-AUS.

Through an Australian Government-aligned procurement process, NEPKI selected DigiCert as its PKI service provider and engaged DigiCert as a PKI expert to support delivery of the national PKI for CSIP-AUS communications.

NEPKI remains the coordinating body responsible for governance and national policy, with DigiCert providing the technical infrastructure and specialist expertise underpinning the service.

NEPKI's objectives:

- Develop, deliver, and maintain a national PKI on a not-for-profit, fair, non-discriminatory basis to facilitate the expeditious and secure adoption of Consumer Energy Resources in Australia
- Procure and manage the PKI for the benefit of PKI Consumers
- Own, operate, and control computer systems, data, and security devices used in connection with the operation of PKI
- Establish arrangements for, and provide access to, PKI for PKI Consumers on a fair and non-discriminatory basis
- Develop and promote cyber safety and asset interoperability in support of the principle of lowest cost for electricity consumers
- Support national consistency for Consumer Energy Resources during the energy transition
- Develop and manage the PKI certification framework for Consumer Energy Resources

What does this mean for CSIP-AUS PKI?

Establish a national Certificate Authority hierarchy
that provides a single root of trust for all energy devices across Australia

Enable secure device registration
so every smart inverter, battery, and controller can be verified before connecting to the grid

Support the CSIP-AUS standard
by providing the PKI infrastructure required for IEEE 2030.5 communications between devices and distribution network operators

Create an open membership model
that allows DNSPs, manufacturers, aggregators, and platform providers to participate under consistent rules

Coordinate with international standards
to ensure Australian energy devices can interoperate with global frameworks as the market evolves

NEPKI is supported by the Australian Renewable Energy Agency (ARENA) and included in Australia's Energy Ministers' CER Roadmap, showing the Australian governments' recognition that digital trust infrastructure is as important to the energy transition as the physical infrastructure itself.

Purpose-Built for Devices: Why DigiCert

Delivering PKI at national scale for millions of energy devices requires a Certificate Authority with deep experience in device identity, operational technology, and critical infrastructure.

DigiCert ONE's Device Trust Manager is a purpose-built platform designed specifically for the challenges NEPKI faces:

Scalable certificate lifecycle management: Automated provisioning, renewal, and revocation of digital certificates across millions of devices, from factory floor to field deployment.

Standards-based architecture: Native support for IEEE 2030.5, the protocol underpinning CSIP-AUS, ensuring compatibility with Australia's regulatory framework from day one.

Hardware-anchored identity: Integration with Trusted Platform Modules (TPMs) and secure elements to bind certificates to physical devices, preventing cloning or credential theft.

Multi-tenant hierarchy: Support for complex trust hierarchies where a national root authority (NEPKI) delegates certificate issuance to individual DNSPs while maintaining centralised policy control.

Real-time revocation and monitoring: Instant revocation of compromised certificates across the entire fleet, with continuous monitoring for anomalous device behaviour.

Post-Quantum Cryptography (PQC) readiness: DigiCert ONE already supports the NIST-standardised post-quantum algorithms ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205), enabling organisations to begin hybrid certificate deployments today. This ensures that energy infrastructure certificates issued now can transition to quantum-resistant cryptography without requiring a full re-architecture, protecting long-lived grid assets against future quantum computing threats.

About DigiCert

DigiCert is one of the world's leading providers of digital trust, securing the connections and communications that underpin the most critical systems in every industry.

DigiCert's digital trust infrastructure is relied upon by:

- **90% of Fortune 500 companies** for TLS/SSL, code signing, and identity management
- **The U.S. Next Generation 911 (NG-911) system** as the root Certificate Authority for emergency communications infrastructure
- **DirectTrust TEFCA health information exchanges** enabling secure clinical data sharing across the U.S. healthcare system
- **The SAE ITC EVPKI Consortium** providing the signing infrastructure for the global EV charging trust list
- **The CA/Browser Forum** as a trusted root distributed and relied upon by every major browser, operating system, and device platform worldwide

DigiCert ONE is a modern, cloud-native platform that consolidates certificate lifecycle management across TLS, code signing, device identity, and document signing into a single operational framework. DigiCert Device Trust Manager, the component most relevant to NEPKI, manages the complete identity lifecycle for connected devices at any scale.

About NEPKI

NEPKI (National Energy Public Key Infrastructure) is established to develop, deliver, and maintain a national PKI on a not-for-profit, fair, non-discriminatory basis to facilitate the expedience and secure adoption of consumer energy resources in Australia and procure and manage a national digital identity framework for Australia's energy sector.

In July 2025, NEPKI received conditional authorisation from the Australian Competition and Consumer Commission (ACCC) to procure and implement a national PKI service for managing secure communication between consumer energy resources and parties in the energy grid. NEPKI's establishment was supported by stakeholders across the energy sector including government organisations, distribution network operators, retailers, device manufacturers, aggregators and peak bodies.

NEPKI operates under an open membership model, enabling anyone in the consumer energy resources sector to participate under consistent governance and technical standards. The framework is designed to scale from current pilot programs to full national coverage as Australia's distributed/consumer energy resource fleet continues to grow.

Beyond NEPKI's initial authorisation and initial objectives relating to distribution network operators securely communicating with energy devices, its core principles, independent governance, and purposeful technical design ensure it is fit for purpose for the whole energy industry and a broader set of use-cases. For example, Electricity Retailers or Virtual Power Plants communicating with devices and/or Electric Vehicles.

The Time to Act Is Now

Australia has an opportunity to lead the world in securing its energy transition. The technology exists. The international regulatory momentum is building. The risks of inaction have been demonstrated.

NEPKI and DigiCert are ready to work with distribution network operators, device manufacturers, energy retailers, aggregators, and government agencies to build the digital trust infrastructure that Australia's smart grid requires.

NEPKI received funding from the Australian Renewable Energy Agency (ARENA) as part of the ARENA's Advancing Renewables Program. The views expressed herein are not necessarily the views of the Australian Government, and the Australian Government does not accept responsibility for any information or advice contained herein.

Next Steps

NEPKI:

Visit nepki.com.au or contact NEPKI at info@nepki.com.au to discuss membership, technical integration, and pilot participation.

DigiCert:

Contact your DigiCert representative or visit: digicert.com/solutions/security-solutions-for-device-trust to learn more about Device Trust Manager and how it supports NEPKI's national framework.

Endnotes

- Australian Energy Market Operator (AEMO), Integrated System Plan 2024. https://aemo.com.au/energy-systems/major-publications/integrated-system-plan-isp
- Clean Energy Council, Clean Energy Australia Report 2025. https://www.cleanenergycouncil.org.au/resources/resources-hub/clean-energy-australia-report
- European Parliament, Regulation (EU) 2024/2847 Cyber Resilience Act, 2024. https://eur-lex.europa.eu/eli/reg/2024/2847/oj
- European Parliament, Directive (EU) 2022/2555 (NIS2), 2022. https://eur-lex.europa.eu/eli/dir/2022/2555/oj 5European
- Parliament, Regulation (EU) 2022/2554 Digital Operational Resilience Act (DORA), 2022. https://eur-lex.europa.eu/eli/reg/2022/2554/oj
- ISO 15118-2:2014 and ISO 15118-20:2022, Road vehicles — Vehicle to grid communication interface. https://www.iso.org/standard/55366.html
- SAE International, ITC EV PKI Consortium Certificate Trust List, November 2025. https://www.sae.org/works/committeeHome.do?comtID=TEVPKIC
- U.S. Food and Drug Administration, Cybersecurity in Medical Devices, 2023. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions
- Connectivity Standards Alliance, Matter Specification 1.4, 2024. https://csa-iot.org/all-solutions/matter/
- Energy and Climate Change Ministerial Council. National CER Roadmap: Powering Decarbonised Homes and Communities. July 2024. https://www.energy.gov.au/sites/default/files/2024-07/national-consumer-energy-resources-roadmap.pdf
- Energy and Climate Change Ministerial Council. National CER Roadmap: Powering Decarbonised Homes and Communities. July 2024. https://www.energy.gov.au/sites/default/files/2024-07/national-consumer-energy-resources-roadmap.pdf