Rheem Australia Pty Ltd ABN 21 098 823 511

Energy Security Board
Level 15, 60 Castlereagh St
Sydney NSW 2000
Submission by email to: info@esb.org.au

16 November 2022

Rheem CET response to the
"Energy Security Board Interoperability Consultation Paper"

Thank you for the opportunity to provide feedback to the "Energy Security Board Interoperability Consultation Paper".

This is a joint response on behalf of both Rheem Australia Pty Ltd (Rheem) and Combined Energy Technologies Pty Ltd (CET), as we have a complementary interest in the Consultation Paper due to the significant number of IES installations we carry out every year in Queensland.

As the largest Australian manufacturer of water heaters with products in over 4 million Australian homes, Rheem offers a wide range of traditional and renewable energy water heater models to the domestic water heating market under the Rheem, Solahart, Vulcan, Aquamax & Everhot brands. Under our Solahart brand we are the third largest supplier of photovoltaic (PV) systems in the country. Over the last four years we have also commenced the manufacture and installation of smart electric water heaters, controlled remotely by our technology partner, Combined Energy Technologies.

Combined Energy Technologies is an Australian technology company specialising in energy management for residential, commercial, and microgrid systems. CET provides site energy management systems and has extensive experience in the integration and orchestration of systems with multiple Consumer Energy Resources (CER), including the integration of solar PV, batteries, water heating, electric vehicle chargers, pool pumps and A/C for the benefit of the homeowner, retailer, and the grid.

References in this letter to CER assets refer to both generation and flexible load, unless specified otherwise. However, our responses to the consultation questions related to CER should be read to include only inverter-based CER assets (defined under AS4777.2:2020) as required to be controlled by CSIP-Aus (the focus of this consultation paper) in the delivery of DNSP flexible exports.

Together, Rheem and CET are already actively participating in the emerging CER market with thousands of online, mixed, orchestrated CER sites across the NEM and the WEM, with near 100% of our sites orchestrating one or more types of CER. Over the past decade we have identified and resolved many issues (at live field sites) to ensure that mixed, smart CER sites can be orchestrated to achieve the best financial outcomes for consumers, whilst providing a foundation for grid support services and hence grid security of supply.

If the energy market is to be truly democratised, it is extremely important that any changes to market rules and associated technical specifications are made with the consumer at the centre of the solution. This will ensure that households continue to invest in smart CER. Fundamental to this approach will be that new rules do not favour a particular technology, technology class, or technology manufacturer, and that technology neutrality is not impeded by barriers to entry in creating or modifying energy market rules. Our specific comments and the recommendations attached are underpinned by this approach.

As Australian based manufacturers, we have made large R&D investments in bringing to market cost effective CER products and technology for the integration and orchestration of CER behind the meter. Further we have a desire to ensure technology neutrality, support for standards, commercial fairness, and adherence to the principles of the NEO in the design of new market services and regulations.

Our comments and recommendations in our feedback are also supported by empirical data from an existing fleet of thousands of consumer sites of mixed CER under orchestration across the NEM and WEM. The data from these sites support our technical, architectural, and commercial positions in our feedback to the Energy Security Board Interoperability Consultation, which we believe are in alignment with the principles of the National Electricity Objective (NEO).

In responding to the Consultation, we have made recommendations and raised questions including:

- That DNSP CSIP-Aus flexible export CER compliance requires all CER to support the CSIP-Aus "Native model" of connectivity regardless of the initial implementation model. This would avoid consumer CSIP-Aus lock-in to only a CSIP-Aus cloud model of connectivity.
- That Domains 3 and 2 should be given equal priority given the interdependence of these two Domains and the need to avoid consumer CER lock-in. This would build consumer trust, ensuring the consumer's investment in their CER asset can be leveraged in a competitive, open marketplace. It would also ensure that services provided by consumer CER assets to DSNPs and AEMO are optimised in their delivery of grid security of supply services.
- That we support a National PKI Certificate Authority, with AEMO being the most relevant authority for this task.
- That we support a nationalised CSIP-Aus product certification process alongside a more robust set of Governance arrangements that includes enforcement of standards compliance (such as for AS4777.2:2020) and a mechanism for product delisting. This should be led by the AER, policed, and enforced through DNSP connection agreements.
- Until Domain 2 interoperability for CER is mandated, we would encourage the ESB to recommend that Government CER rebate programs have a requirement for CER product compliance to locally accessible interoperability to avoid consumer CER lock-in. In the interim this requirement could be based around California Rule 21, under the 2023 requirement for CER to support SunSpec Modbus per IEEE1547. This limits any additional compliance costs on manufacturers for products sold in Australia.

As this submission has been prepared using the expertise of several of Rheem and CET personnel, I would ask that any enquiries related to the submission are directed in the first instance to myself. I will then co-ordinate follow up responses to your enquiries or further meetings with the appropriate personnel within our organisations.

Yours Sincerely

Ashraf Soas
General Manager Energy Solutions
Rheem Australia Pty Ltd

ashraf.soas@rheem.com.au
M: +61 417 061 380

Rheem CET responses to the ESB Interoperability Consultation questions

Q1 Are the five identified domains correctly summarised? Are there gaps or major limitations in this framing?

The five identified domains are broadly correctly summarised. However, for the domains to deliver their stated purposes there is necessary crossover and dependencies between the domains. For example, Domain 3, i.e. CSIP-Aus cannot be effectively implemented for multi-CER sites (the CSIP-Aus gateway model) without the implementation of Domain 2 BTM Interoperability supporting it. Further, if we are to avoid consumer lock in, the implementation of Domain 3, i.e. CSIP-Aus, requires that all CER supports the CSIP-Aus native model regardless of whether the cloud model is the initial deployment model used at a site. That is, the consumer should be able to churn their CER asset between the different technology connectivity models (refer ESB Interoperability Policy Document Figure 6: Supported technology models) to use the energy market service provider of their choosing, and/or as they add CER to their site that will require re-configuration to support the CSIP-Aus gateway model. Under the gateway model the ideal scenario would be full support by CER of Domain 2 interoperability (e.g. support for SunSpec Modbus as per California Rule 21 and the 2023 requirement for SunSpec Modbus support under IEEE1547, as an example). That however does not preclude the requirement to support the native model on a single DER site where the consumer wishes to churn a single CER asset from the cloud model to the native model, thus avoiding CER lock in. Hence all CER should support the native model as a minimum requirement.

These underlying technical prerequisites of particular domains required to enable the outcomes of other domains need to be taken into account in assigning the domain priorities. We address this further in our responses to the consultation questions.

Q2 What priority should each domain be assigned, considering the interest of all electricity consumers within the consumer energy resource interoperability landscape?

In considering the priority to be assigned to each domain, the consumer should be at the centre of any decisions. Consumers are making buying decisions and deploying CER assets now, especially solar PV systems and battery energy storage systems (BESS).

In our experience consumers are largely uninformed at the point of purchase of CER assets, and reliant on the CER vendor to inform the consumer regarding the capabilities and any limits or restrictions (technical and/or commercial) that may be inherent in their CER asset purchase. Unfortunately, CER sales are not closely regulated, and the consumer is rarely informed of technical and commercial limitations during the CER purchase process. This is resulting in CER asset lock-in, particularly in the BESS space.

We believe that a key issue for resolution under this consultation is to set rules that will allow consumers to leverage their CER asset with the energy market service provider of their own choosing in a competitive, open marketplace. This will ensure that no provider has preferential access to features and performance of the consumers CER asset due to commercial arrangements with the CER manufacturer, and that the consumer is not restricted in churning to only those providers with commercial agreements with the CER manufacturer. This then expands the remit of interoperability beyond just the availability of a standards based local control interface, supporting an open communications protocol for a set of commands and responses. For a truly competitive market, interoperability should also define the full feature set and command response times of the CER asset such that no energy market service provider has preferential access to more features and a higher level of performance of the consumers CER asset. The only exceptions to this principle being restrictions around access to fundamental asset specific safety and performance controls – customer safety and customer amenity must not be compromised by incompetent management of their assets.

Our field experience from many thousands of mixed CER sites across the NEM and WEM proves that consumers have the most flexibility in how and with whom they monetise their CER asset when that CER asset supports the aforementioned minimum requirements for local, open access and control - *this is Domain 2 – "Behind the Meter" interoperability".*

Whilst the current focus of this policy consultation is on the DNSP implementation of CSIP-Aus for flexible exports, the CSIP-Aus models of connectivity currently allowed by those DNSPs implementing flexible exports will enable vertical monopolies to be built. This may result in consumer technical lock-in to particular CER, and commercial lock-in of that CER with only those retailers that have a commercial arrangement / relationship with the particular CER manufacturer.

This consumer lock-in manifests itself, for example, where the consumer unknowingly purchases CER that only uses the CSIP-Aus cloud model connectivity option (refer consultation document Figure 6: Supported technology models – Cloud model). The cloud model uses a proprietary connection from the cloud to the consumer's CER on the consumer's site. Where the CER only supports the proprietary cloud model connectivity option, the consumer is precluded from churning their CER asset to a provider that supports alternate CSIP-Aus pathways such as the direct client (native model) or the gateway client (gateway model). In the case of the gateway model, a lack of Domain 2 interoperability at the CER device level creates further problems in the orchestration of multiple CER on the consumer site to conform with a single CSIP-Aus connection to the site / NMI as required by the DNSP.

It is our recommendation that all inverter-based CER should support a client level (on the inverter) CSIP implementation (i.e. the native model) regardless of the CSIP-Aus model of the initial deployment. This will ensure consumers are not adversely affected financially and they are not locked-in.

Where DNSPs are accelerating the requirement for flexible exports (such as by mandate) and are allowing a proprietary CSIP-Aus cloud model without a requirement for the CER to support the native model, the DNSPs are enabling and accelerating further consumer lock-in of their CER assets.

A valid question here may be:

Who should be responsible for informing the consumer that their CER asset purchase may result in them being locked-in technically and / or commercially for the life of that CER asset?

In the absence of changes to the allowable CSIP-Aus connectivity models, this consumer CER lock-in issue needs to be highlighted to the consumer during their deliberation process for the purchase of their CER asset. The development of a CER whitelist may be needed to inform consumers, however this would require the development of a definition of a CER as interoperable for the purpose of CSIP-Aus, and how this may relate to an interoperability standard (Domain 2) for behind the meter CER orchestration. Overseas jurisdictions are already addressing this issue. For example, as a result of California's Rule 21 and the SunSpec organisation's work around CSIP and BTM interoperability, nearly all manufacturers of inverter-based CER products support the SunSpec Modbus protocol. With the exception of a few inverter-based CER, the industry has by default accepted Modbus as an open protocol for local BTM connectivity and control. This approach is further supported in California whereby mandatory support for local BTM interoperability on inverter-based CER will come into force in 2023 under IEEE1547. Further, as nearly all inverter-based products support remote upgrade capability, it is then only regulatory / commercial considerations that stand in the way of enabling BTM interoperability on currently deployed consumer CER to remove consumer CER lock-in.

Based on the above, we believe that the order of priority of the domains should be as follows:

Recommended Domain Priority List:

- Domains 3 and 2 = equal priority, given the interdependence of these two domains and the need to avoid consumer lock-in. This then builds the foundation for the other domains and builds consumer trust by ensuring the consumer's investment in their CER asset can be leveraged in a competitive open marketplace.
- Domains 4 and 5 = equal priority. Solving interoperability within Domains 3 and 2 ensures that services provided by the consumer CER assets to DSNPs and AEMO are optimised to deliver grid security of supply.
- Domain 1 – Interoperability for this domain requires the greatest thought, and we believe learnings from projects such as the AEMO Edge Project will best inform the interoperability requirements of Domain 1.

Specific CSIP-Aus Recommendation

It is our recommendation that all inverter-based CER should support a client level (on the inverter) CSIP-Aus implementation (i.e. the native model) regardless of the CSIP-Aus connectivity model of the initial deployment. This will ensure consumers are not adversely affected financially and that they are not locked-in to any manufacturer or retailer for the control of their CER asset.

Making CSIP-Aus native model a default requirement will ensure that a consumer can add CER to their site, and will facilitate their future transition to the CSIP-Aus gateway model to orchestrate all CER on their site via a single CSIP-Aus connection per site / connection point. This does not preclude an initial cloud model or a native model implementation, rather it enables consumer choice in service provider and CER asset market participation.

Q3 What are the likely costs and benefits for consumers associated with a national 'flexible export ready' mandate including in relation to future readiness of customer installations and installation costs?

Referring to our answer to Question 2, the costs, and benefits (or lack thereof) to consumers may vary considerably, dependent on how and when the national 'flexible export ready' mandate is implemented. Rheem believes that this is directly related to the extent of CER compliance with both Domain 2 behind the meter interoperability and as detailed for Domain 3, the need for CSIP-Aus support/compliance at a device level (native model), irrespective of the initial deployment configuration model. Please see our response to Question 2 above for more details.

In the absence of CER supporting Domain 2 interoperability, there are also issues with the use of basic CER control mechanisms (and unnecessary costs to consumers) to implement a national 'flexible export ready' mandate on multi-CER sites. In order to conform to a flexible export limit on multi-CER sites where one or more CER does not support local interoperability, DNSPs have sanctioned the use of DRM0 (Demand Response Mode Zero), an on/off grid disconnect mechanism called up under AS4777.2:2020, as a mechanism to control site export. However, as there is widespread deployment of CER in the market with no support for this mandatory AS4777.2:2020 requirement, additional costs on consumers will arise. These additional costs extend to installation and equipment costs, along with site enablement complexity in the control of the non-compliant CER. In the absence of DRM0, a typical solution is to install a relay in the power supply circuit of the CER, for flexible export compliance. This is not an ideal solution moving forward. We have also raised this example as an AS4777.2:2020 compliance, policing and enforcement issue, both within this response and within our response to the AEMC Review into CER Technical Standards.

Use case examples of costs and associated issues:

Referring to Figure 6 of the *Interoperability Policy Directions Paper - Supported technology models*. Whilst the cloud model should not be precluded as a supported technology model, the consumer's CER asset (inverter) should be capable of churning between the three models (native, gateway and cloud) at the discretion of the consumer, avoiding CER lock-in.

Where CER supports local BTM orchestration via standards-based interfaces and open control protocols (Domain 2 interoperability), and the flexibility of a device level (native model) CSIP-Aus implementation, then it naturally flows that the costs to the consumers for compliance with a flexible export ready mandate and/or participation in other grid services are minimised.

In support of this recommendation, our own experience as a Tier 1 installer of solar PV and BESS across the NEM and the WEM indicates a growing number of sites deployed with multiple inverter-based CER technology. For example, as the solar PV installation and connection rules evolve over time, it is generally not viable to upgrade an existing solar PV system and the customer often elects to install a second or even third solar PV system.

Issues arise on these sites when installing multiple solar PV systems where there is an existing CSIP-Aus flexible export connection that is using the cloud model - ref Figure 6 of the *Interoperability Policy Directions Paper* (i.e., the inverter is connected to the cloud via a proprietary communication means) and there is no local support for the CSIP-Aus native model.

Under the above scenario the installation of a second solar PV system requires the site to comply with the DNSP requirement for a single CSIP-Aus pathway per site (home) / NMI. In these cases, we install a site edge gateway (HEMS) in accordance with the CSIP-Aus gateway model of Figure 6 of the *Interoperability Policy Directions Paper - Supported technology models*. As the gateway is the CSIP-Aus compliant device for the site, the new solar PV inverter must sit behind the gateway, with the gateway executing the CSIP-Aus commands, via translation to a Modbus command which is supported by the solar PV inverter.

Where the existing solar PV inverter is using a proprietary connection to a cloud, i.e. the CSIP-Aus cloud model, we must transfer CSIP-Aus site compliance of this inverter to the gateway to maintain site orchestration BTM of all the inverter based technology, and hence a single CSIP-Aus path to the site (home)/ NMI as required by the DNSP. For the existing cloud model solar PV inverter connection, the options are:

a) Bring the existing cloud model solar PV inverter into the gateway orchestration as per the new inverter, or;

b) Where the existing cloud model solar PV inverter does not have a local standards-based interface, nor support an open protocol such as Modbus, we would need to use the DRM0 interface on the solar PV inverter for simple on/off control via a relay (in the power circuit to the inverter) under the control of the site edge gateway (HEMS).

Such an implementation is a sub optimal and costly solution for the consumer, further enabling and accelerating consumer lock-in because of the way the supported technology models of CSIP-Aus are being implemented by the DNSPs. This will further erode consumer confidence, resulting in missed market participation opportunities, and eventually large capital costs being imposed on consumers in the replacement of their closed CER asset purchases.

AEMO and DNSP grid security of supply imperatives are rightly driving the requirement to accelerate flexible export / dynamic connection initiatives. However, without careful consideration to ensure that CER interoperability (both CSIP-Aus and BTM) is a foundational requirement of DNSP flexible export / dynamic connection initiatives, there will be impacts to consumers and the grid. These impacts include short- and long-term costs associated with technical and commercial lock-in of consumers unable to orchestrate their CER assets BTM, nor leverage their CER assets with the energy market service provider of their choosing.

A further area that needs to be addressed is that of Government sponsored CER subsidy programs that are causing hidden consumer costs due to lock-in. This is because there are no prerequisite technical and commercial requirements of these subsidy programs for program approved CER to support open, local interoperability and commercial neutrality.

As an example, please refer to the Engage Victoria (see : https://engage.vic.gov.au/protecting-consumers-of-der) technology guidelines principles (see: https://www.solar.vic.gov.au/technology-guidelines) *Guiding Principle 06 - Promote interoperability through enhanced communications* within the document.

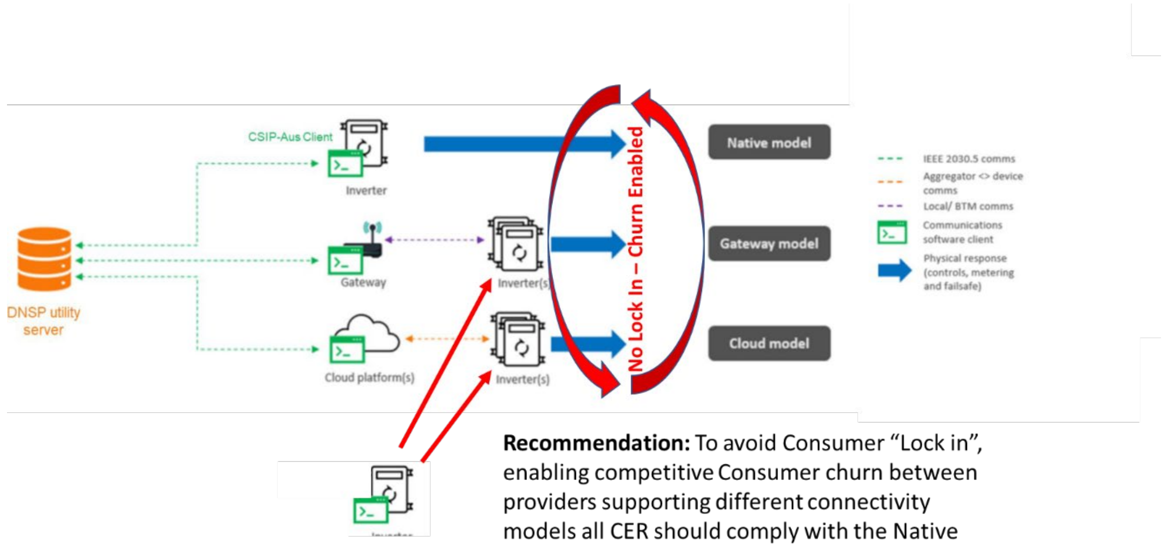
These guiding principles have not been a requirement for manufacturers wishing to participate in the current Victorian government battery subsidy program. The consumer is likely to be unaware that their purchase has further enabled proprietary Cloud only connected battery solutions that:

a) do not support interoperability / do not have local interfaces on the battery for a HEMS to orchestrate the BESS with other consumer CER – causing the consumer financial loss where the uncontrolled BESS CER fights for solar self-consumption resources and impacts grid security of supply when the BESS CER fights with other CER providing grid services.

b) enables consumer lock-in both technically and commercially as the consumer cannot choose the energy market service provider they wish to use and can only use the retailer that has an agreement with the CER inverter manufacturer, if they want to monetise their inverter (typically BESS) asset.

Recommendation:

Referring to the diagram below we have provide a suggested enhancement to the supported CSIP-Aus technology models. To avoid consumer CSIP-Aus CER lock-in and hence build the foundation for competitive consumer churn, we recommend that all inverter based CER should support as a minimum the CSIP-Aus native model of connectivity regardless of the initial deployment model. This does not preclude use of the cloud model but does enable the consumer to churn their CER asset to an energy market service provider offering the native model of connectivity or the gateway model of connectivity. (Where in the absence of Domain 2 CER interoperability the Gateway acts as both a CSIP-Aus client and a BTM CSIP-Aus server). Failure to implement this enhancement will further propagate consumer CER lock-in (i.e. no churn between CSIP-Aus models possible), restricting the ability of the consumer to add and orchestrate multiple CER in compliance with a dynamic connection.



Recommendation: To avoid Consumer "Lock in", enabling competitive Consumer churn between providers supporting different connectivity models all CER should comply with the Native Model (embedded CSIP-Client) as a minimum regardless of the initial deployment model.

Diagram 1: Suggested enhancement to the supported CSIP-Aus technology models

Q4 Do stakeholders agree that DNSPs are best placed to enforce a 'flexible export ready' mandate at the time of installation? If not, what alternative models should be considered?

As we have detailed in our answer to Question 15, enforcing a 'flexible export ready mandate' requires a robust governance arrangement around the listing and delisting of CER products that are non-compliant despite their certification listing (AS4777.2:2020, CSIP-Aus etc). In looking at how government might enforce a 'flexible export ready' mandate through CSIP-Aus compliance, Rheem believes that lessons can be drawn from existing issues with CER compliance.

For example, a fundamental issue to address is ensuring that CER shipped and deployed in Australia complies with its Certificate of Compliance to AS4777.2:2020. Currently no robust mechanism for policing and enforcing compliance with AS4777.2:2020 exists, and whilst the CEC does maintain a whitelist (on a self-managed basis) of CER certification (primarily in respect to AS4777.2:2020), the CEC has no role in the investigation of complaints that equipment imported and deployed does not meet its own Certificate of Compliance with AS4777.2:2020.

This and other non-compliances are most likely to be revealed at the time of initial CER installation by installers and systems integrators requiring compliance with DNSP connection agreements. Hence for compliance and enforcement the DNSPs are the best place for this obligation to reside, supported by their connection rules. It is here that DNSPs can play a greater role through their inspection and defect notification / rectification processes, whereby CER product reported as being non-compliant is investigated by the DNSP, and where confirmed, the DNSP defect tagging and defect rectification processes can be applied. However, field experience suggests an unwillingness by DNSPs to pursue non-compliances unless there is an immediate safety related issue. This gap needs to be addressed to ensure an effective governance arrangement around the listing and delisting of CER with regulatory backing. We believe that a nationally consistent approach is required here, and that the AER is currently the most appropriate body, acknowledging that the AER may need new powers to direct DNSPs. Longer term a new national consumer energy resource technical regulator may be a more appropriate body, however in the short term we urgently need the issue of non-compliance addressed. Only then can the enforcement of a 'flexible export ready' mandate be considered.

Further, how Domains 2 and 3 are implemented (Refer to our response to question 2 & 3 above) will affect the extent to which a site is capable of being 'flexible export ready', particularly in the case of multi-CER sites.

Q5 What requirements should a 'flexible export ready' installation have with regard to internet connectivity (e.g. embedded mobile communication versus LAN connectivity)?

A 'flexible export ready' installation should be agnostic to the connectivity technology.

That is, different installations may be more suited to different communications technology. Site connectivity might be mobile communications, NBN fibre, powerline mesh communications to a grid concentrator / hub etc. Site connectivity may change by provider, may have multiple paths (trader and DNSP) but in all cases any 'flexible export ready' installation should be designed in and around the switchboard to support future communications technology changes.

At a minimum, supporting industry standard IP (TCP/IP), which is the ubiquitous standard for communications regardless of the physical interconnection technology used, will future proof an installation.

Q6 What are the pros and cons of a flexible export ready mandate set in the Rules, via a subordinate instrument, or under a separate head of power (e.g. jurisdictional technical regulation)?

On February 25, 2021, the AEMC issued a rule determination (Rule 2021) for "Technical Standards for Distributed Energy Resources". The final rule included a reference to AS4777.2:2020 (as updated) to create jurisdictional consistency and uses the existing framework for embedded generator connections in Chapter 5A of the NER. Further, the final rule places an obligation on DNSPs to ensure that:

"if the connection applicant is proposing to connect a new or replacement embedded generating unit by way of a basic micro EG connection service, that the embedded generating unit the subject of the connection application is compliant with the DER Technical Standards."

We believe that the "Rules" is the right place for a flexible ready mandate, as this will maintain jurisdictional consistency, enables a national approach to implementation of CSIP-Aus and sets up a framework for the inclusion of other interoperability domains beyond Domain 3 CSIP-Aus.

However, our experience has been that despite there being an obligation placed on DNSPs by the AER in respect to AS4777.2:2020 compliance, there has been an unwillingness to investigate reported non-compliance of CER product with the AS4777.2:2020 standard / product certification issued against the standard. Our empirical evidence from many thousands of BTM orchestrated CER sites shows that the ability of a customer to respond to a flexible export (or import) limit is directly affected by the location of the communication client as supported in a CER per the CSIP-Aus connectivity models.

Therefore, there needs to be (as a priority) an oversight mechanism for policing and enforcement of product compliance with AS4777.2:2020. The success or otherwise of a flexible export ready mandate will be heavily reliant of DER/CER compliance with the AS4777.2:2020 standard. This is particularly relevant to the success of a flexible export mandate when implementing the gateway model of CSIP-Aus on multi-CER sites. The currently proposed connection pathways of the three CSIP-Aus models (native, gateway and cloud) do not require CER to support as a minimum the native model, hence a consumer that is only offered a cloud model connectivity option may find themselves unable to later churn their CER asset to the native model or gateway model, hence they become locked-in.

The only viable option to maintain CSIP-Aus compliance on a multi-CER site implementing a flexible export is then via the CSIP-Aus gateway model, which enables orchestration of multiple CER behind the meter. In the absence of the CER supporting either Domain 2 interoperability or the CSIP-Aus native model (i.e. the CER only supports the CSIP-Aus cloud model) the only control option for orchestration behind the site Gateway is on/off control via the CER DRMO interface. However widespread lack of compliance (under AS4777.2:2020) with mandatory DRM0 precludes this option.

For the reasons given above we believe the Rules is the logical place for enforcement and compliance with a flexible export ready mandate given that AS4777.2:2020 is already embedded in the Rules. But this must be backed by an effective mechanism for the policing and enforcement of product compliance with AS4777.2:2020.

Further, we believe that DNSP CSIP-Aus certification must include a requirement for mandatory support of the CSIP-Aus native model irrespective of the connectivity model utilised during an initial installation. This would ensure that the consumer is not locked-in to a particular energy market service provider for their implementation of a flexible export mandate and the consumer is free to move their CER assets between the three CSIP-Aus connectivity models (native, gateway and cloud).

Q7 If implemented under the Rules, which market body is best placed to establish and oversee the proposed requirement on DNSPs?

The AER is a logical choice to establish and oversee the proposed requirements on DNSPs, however per our answer to Question 6, the AER has been unable to police and enforce (via DNSPs) mandatory technical requirements of AS4777.2:2020 certification, which raises concerns for any oversight of CSIP-Aus compliance. Further, and as raised in our answer to Question 6, an example of this regulatory enforcement gap is the widespread lack of compliance (under AS4777.2:2020) with mandatory DRM0 capability, support of which is a requirement on behind the meter micro embedded generating units to enable an alternate emergency disconnect / shutdown of the inverter (solar PV or battery). For example, this capability is used to enable safe disconnection by Building Management Systems (BMS – e.g. when fire systems are triggered) and by Home Energy Management Systems (HEMS - e.g. in conjunction with smoke alarms etc). The necessary changes to rules and regulations (if that is what is required) must be made to ensure that the entity assigned (whether the AER or another dedicated, new market body) to oversee the proposed compliance requirements on DNSPs, has a well-developed governance process for policing and enforcement.

Q8 What are the pros and cons of a flexible export ready mandate referring to CSIP-Aus in Standards Australia Handbook form?

This would be consistent with a Rules based national approach to a flexible export ready mandate and supports the current progress of the CSIP-AUS implementation guide through Standards Australia to be made into a technical handbook.

With no current process underway to develop CSIP-Aus as an Australian standard we see it as being essential that regulatory instruments such as the NER can be used to call up compliance with CSIP-Aus as a Standards Australia Handbook, however equally important is an effective governance arrangement around the delisting of non-compliant CER product.

Q9 Would there be value in agreeing a national approach to public key infrastructure for consumer energy resources?

Yes, a single entity / national approach (NEM and WEM) should be put in place for PKIs for consumer CER.

Q10 Are there existing examples that could be used as a model for the consumer energy resources ecosystem?

Yes. Services Australia manages Public Key Infrastructure (PKI) certificates for health professionals to enable secure access to online services such as Medicare.

See: https://www.servicesaustralia.gov.au/public-key-infrastructure

Q11 What are the pros and cons of establishing a national certificate authority?

A national certifying authority would provide a higher level of security, one technical implementation, one issuing authority, making it easier to regulate the certificate implementation costs, assuming that AEMO or other AEMC endorsed entity held the role of National Certificate Authority).

Q12 Do stakeholders have a view as to who should perform the role of national certificate authority, if it were created?

This could be either a government entity, a newly created entity responsible for CER, or preferably the Australian Energy Market Operator (AEMO).

AEMO seems like the current logical choice given that they already have the 24/7 secure systems, the required software platforms (including redundancy) and the required processes (both technical and governance) in place that would be necessary to issue and support the PKI infrastructure for CER certificates. The SunSpec model (Kyrio issuing the certificates) requires all CSIP testing and compliance to be carried out by SunSpec, excluding market competition. Whilst SunSpec is a member organisation and that model may be suitable to the Californian market, AEMO as the certificate authority makes more sense. Further AEMO as National Certificate Authority for PKI would not preclude the use of certified test labs and hence market competition for CSIP-Aus testing / compliance services, as is the current status with AS/NZS standards.

Q13 What views do stakeholders have about the adaptability of existing industry-led product certification and compliance processes for future use?

We agree that:

"Further work is required to develop an effective governance arrangement around the listing (and delisting) process. The ESB considers that this arrangement must ensure transparent and fair treatment of OEMs, with appropriate incentives and penalties to ensure that products being installed are consistent with those listed. A compliance program would be required to enable non-compliant

products to be identified (e.g. by networks, installers, consumers or competitor OEMs). A key incentive in this framework would be the threat of product-delisting however, interim penalties and make-good arrangements should also be considered."

As we have detailed in our answers to Questions 14 and 15 below, whilst the CEC does maintain a whitelist (on a self-managed basis) of CER certification (primarily in respect to AS4777.2:2020), they have no role in the investigation of complaints that equipment imported and deployed does not meet its own Certificate of compliance with AS4777.2:2020. We have raised specific examples of AS4777.2:2020 non-compliance in our answers to Questions 6 and 7 and detailed how there is no guaranteed mechanism of policing and enforcement in cases of non-compliance. As such, whilst product certification via accredited test labs seems to be working well, in our view there exist no robust industry-led product policing and compliance processes. Currently an AS4777.2:2020 certificate of compliance can only be relied on for the sample(s) of CER product that undertook testing. Propagating this issue further with CSIP-Aus makes no sense as there are no governance processes, with guaranteed regulatory backing, for the policing and enforcement processes needed to ensure that CER product shipped and deployed under a particular certificate actually meets the requirements of the certification.

This is a major gap and one that we hope the AEMC will resolve as an outcome of their Review into CER Technical Standards.

Q14 What views do stakeholders have about the most appropriate body to have oversight of the product certification and listing/delisting processes?

As we detailed in our answer to Question 13, whilst the CEC does maintain a whitelist (on a self-managed basis) of CER certification (primarily in respect to AS4777.2:2020) however have no role in the investigation of complaints that equipment imported and deployed in Australia does not meet its own Certificate of Compliance with AS4777.2:2020. This serious governance issue around CER product compliance listing needs to be resolved if we are to expand the CEC's remit to include a CSIP-Aus CER product whitelist.

The CEC product whitelisting simply means that a sample of the CER product listed was tested in an accredited lab and passed all the mandatory requirements of AS4777.2:2020. This trust (by consumers and other energy industry stakeholders) in a CER product compliance certificate is misplaced, as there are no guarantees or processes that ensure the CER product shipped and deployed in Australia actually meets the certification on record. This exposes a large governance gap in the role that the CEC plays as the custodian of CER certifications. Consumers, installers, and the industry in general would most likely be unaware that CER product whitelisted as certified may not actually meet the mandatory requirements of the standard(s) to which it is certified.

Given that AS4777.2:2020 is called up in the NER, it would make sense that CSIP-Aus is also called up in the NER. In the absence of a new national consumer energy resource technical regulator, we believe that the AER is the most appropriate body to have oversight of a product certification and listing / delisting process. However, for any listing /delisting process to be effective, a fundamental issue to address is how to ensure CER shipped and deployed in Australia complies with its Certificate of Compliance to CSIP-Aus, to AS4777.2:2020 etc.

If the AER or another body is tasked with CER product certification listing /delisting processes, then there also needs to be a clear and robust mechanism for non-compliance policing, rectification enforcement, and product recall / delisting. This process should be backed by the NER or other legal instrument that is enforceable on a national basis, with the chosen body suitably equipped to legally enforce compliance and/or issue product recalls and fines as necessary. As detailed in our answer to Question 15 below, non-compliance of CER products with their certification listing is most likely to be revealed at the time of initial CER installation by installers and systems integrators. It therefore makes sense that the DNSPs also have a key role to play to enable the AER with the tools it requires in an enforcement role.

Q15 What role could DNSPs have in the product certification/decertification process in the context of improving outcomes for industry and consumers?

Adding to our answers to questions 13 & 14, DNSPs embed a requirement for compliance with standards such as AS4777.2:2020 and AS/NZS 3000 within their Customer Connection Agreements. This should be expanded to cover CSIP-Aus compliance of participating CER products.

In practice the non-compliance of CER products with their certification listing (AS4777.2:2020, CSIP-Aus etc) is most likely to be revealed at the time of initial CER installation by installers and systems integrators. DNSPs can play a greater role here through their inspection and defect notification / rectification processes whereby CER product reported as being non-compliant is investigated by the DNSP, and where confirmed, the DNSP defect tagging and defect rectification processes can be applied. However, field experience suggests an unwillingness by DNSPs to pursue reported CER standards non-compliances unless there is an immediate safety related issue. This gap needs to be addressed to ensure an effective governance arrangement around the listing and delisting of CER with regulatory backing. Rheem believes that a nationally consistent approach is required here, and that the AER is currently the most appropriate body, acknowledging the AER may need new powers to direct DNSPs. Longer term a new national consumer energy resource technical regulator may be a more appropriate body, however in the short term we urgently need the issue of non-compliance addressed.

Expanding on the DNSP role, where a field rectification is not possible (e.g., the CER product deployed simply doesn’t meet a mandatory requirement of AS4777.2:2020, CSIP-Aus etc, and would require a fundamental change (e.g. new interfaces / electronics) on the product) then the DNSP should have a role in providing such evidence to the AER and making a recommendation of the required remedy to bring the CER product into compliance with its certificate. Where a remedy is not possible, the DNSP should have a regulatory backed role that may include enforcing a product recall and/or decertification with the CER/CEC.

Despite the AER having a role in overseeing DNSP customer connection agreements, and a responsibility for ensuring that networks comply with laws and guidelines, it is the regulatory gap in policing and enforcement of CER to standards that requires immediate action to ensure consumers are adequately protected.

Further, a review of the processes for investigating, policing and enforcement / rectification of CER reported as being non-compliant with a standard such as AS4777.2:2020 is recommended as a matter of urgency.