# Privacy-Preserving Metering for Smart-Grids

*Executive Summary*

*We propose a secure protocol between a customer's electricity meter and a utility provider that* ***reveals the total consumption fee, while keeping private the individual measurements.*** *Furthermore, it* ***guarantees the fee is correct*** *and derived according to the fine-grain meter measurements and the tariff policy of the provider.*

In our system the utility provider sets a tariff policy, signs it and sends it to the user. The pricing policy maps consumption and other parameters such as the time of day, to a tariff. Over the billing period, meters output readings and other metering information and sign them. Periodically, the user, their device or a service of their choice, uses the readings to compute a payment message that includes the total fee and a mathematical proof that the fee is correct, given the applicable tariffs and the readings. Upon receiving the payment message the provider can check the correctness of the bill without learning any information about the individual meter readings.

Additionally, our protocol allows for the selective disclosure of consumption data to the provider, but only with the users' consent. The selective disclosure of fine-grained data is certified to be correct, and other function of readings can be computed and revealed. Besides the final bill other information can be released, such as the total consumption within the billing period, as it is done today, to facilitate network management and fraud prevention.

Security for the provider relies on established signature schemes and the binding property of cryptographic commitments. User privacy relies on the zero-knowledge property of proofs of knowledge and on the hiding property of commitments. The provider ensures that the signatures on the meter readings are correct though tamper-evident hardware as for conventional metering security. Our protocols are proved secure using well established cryptographic techniques.

Users can delegate the calculation of their bill to any device or service they wish (Figure 1): a home server, an on-line service or a smart meter. No matter what their choice is, the provider and everyone else can verify in case of dispute that the final bill is correct, and does not need to trust the actual computation or the party that performed it. The freedom to perform the computation of the bill locally or through any device or delegate, without revealing the detailed readings, allows the user to preserve their privacy.

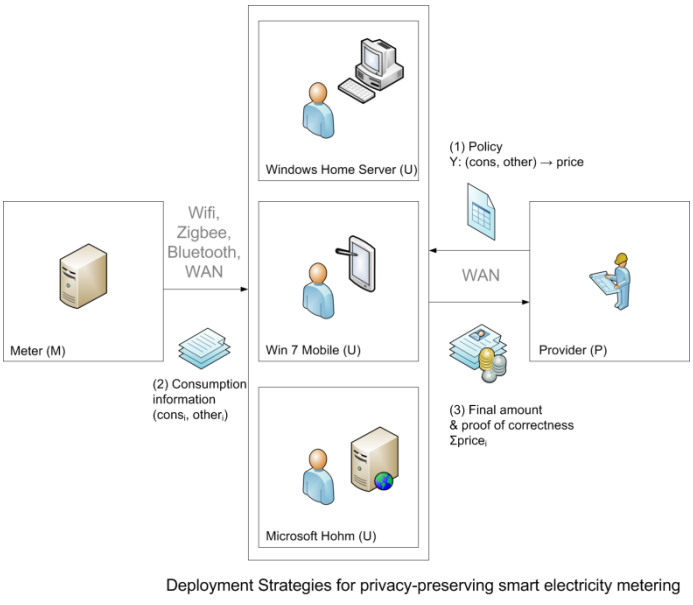


**Figure 1. Deployment**

Our technology combines the benefits of fine grained metering and charging with users' needs for privacy. It is applicable to a number of settings beyond utility metering, such as pay-as-you-drive car insurance, road tolling and taxation, utility billing or software licence management, providing integrity and privacy to any billing process.

***For more information contact:***

*George Danezis, Microsoft Research Cambridge, <gdane@microsoft.com>*
*Alfredo Rial, Microsoft Research & KU Leuven, <alfredo.rial@esat.kuleuven.be>*

Microsoft Research