Digitale Signaturen

Asymmetrische Verfahren wie RSA funktionieren meist spiegelbildlich: Informationen, welche mit dem öffentlichen Schlüssel verschlüsselt werden, können mit dem privaten Schlüssel entschlüsselt werden. Es ist aber auch möglich, eine Information mit dem privaten Schlüssel zu verschlüsseln - diese Information kann dann jeder, der den öffentlichen Schlüssel besitzt wieder entschlüsseln. Was soll das bringen?

Wenn ich eine Nachricht mit dem öffentlichen Schlüssel entschlüsseln kann, kann ich mir sicher sein, dass der Sender im Besitz des privaten Schlüssels ist.